



---

Junos<sup>®</sup> OS

# Complete Software Guide for SRX Series Services Gateways, Release 12.1x46-D10 (Volume 1)

Release

12.1x46-D10



---

Modified: 2016-08-08

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://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<sup>®</sup> OS Complete Software Guide for SRX Series Services Gateways, Release 12.1x46-D10 (Volume 1)*  
12.1x46-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 . . . . .	lvii
	Documentation and Release Notes . . . . .	lvii
	Supported Platforms . . . . .	lvii
	Using the Examples in This Manual . . . . .	lvii
	Merging a Full Example . . . . .	lviii
	Merging a Snippet . . . . .	lviii
	Documentation Conventions . . . . .	lix
	Documentation Feedback . . . . .	lxi
	Requesting Technical Support . . . . .	lxi
	Self-Help Online Tools and Resources . . . . .	lxi
	Opening a Case with JTAC . . . . .	lxii
<b>Part 1</b>	<b>Junos OS Getting Started Guide for Branch SRX Series</b>	
<b>Chapter 1</b>	<b>Overview . . . . .</b>	<b>3</b>
	SRX Series Basics . . . . .	3
	SRX Series Overview . . . . .	3
	Understanding Factory Default Configuration Settings of an SRX210 . . . . .	3
	Default Configuration Topology . . . . .	4
	Default Port Settings . . . . .	5
	Default Settings for Interfaces, Zones, Policy, and NAT . . . . .	5
	Default System Services . . . . .	6
	Autoinstallation . . . . .	6
	Understanding Methods to Manage Your Branch SRX Series . . . . .	6
	SRX Series Security . . . . .	7
	Understanding Branch SRX Series Stateful Firewall Functionality . . . . .	7
	Understanding Security Zones and Policies for SRX Series . . . . .	8
	Zones . . . . .	8
	Security Policy . . . . .	8
	Understanding NAT for SRX Series . . . . .	9
	Understanding Unified Threat Management for Branch SRX Series . . . . .	10
	Understanding Intrusion Detection and Prevention for SRX Series . . . . .	12
	Understanding IPsec VPN for SRX Series . . . . .	12
	Understand Chassis Cluster for SRX Series . . . . .	13

<b>Chapter 2</b>	<b>Configuration</b>	<b>15</b>
	SRX Series Basics	15
	Mandatory Settings to Configure Your Branch SRX Series	15
	Connecting Your Branch SRX Series for the First Time	16
	Connecting Your Branch SRX Series Through the Console Port for the First Time	16
	Configuring System Identification and User Classes for Your Branch SRX Series	18
	Configuring Internet Access for Your Branch SRX Series	18
	Configuring a Network Time Protocol Server for Your Branch SRX Series	23
	Validating Your Branch SRX Series Configuration	23
	Verifying Your Branch SRX Series Configuration	24
	Connecting Your Branch SRX Series Through the Console Port for the First Time	25
	Configuring System Identification and User Classes for Your Branch SRX Series	26
	Configuring Internet Access for Your Branch SRX Series	27
	Configuring a Network Time Protocol Server for Your Branch SRX Series	31
	Validating Your Branch SRX Series Configuration	32
	Verifying Your Branch SRX Series Configuration	33
	SRX210 Factory Default Setting—A Sample	34
	Resetting Your Branch SRX Series	38
	Resetting Your Branch SRX Series	38
	SRX Series Security	38
	Example: Configuring Security Zones and Policies for SRX Series	39
	Example: Configuring Destination NAT for SRX Series	43
	Updating Licenses for a Branch SRX Series	48
	Example: Configuring Unified Threat Management for a Branch SRX Series	50
	Example: Configuring Intrusion Detection and Prevention for SRX Series	53
	Configuration Statements	57
	Security Configuration Statement Hierarchy	58
	[edit security address-book] Hierarchy Level	59
	[edit security policies] Hierarchy Level	59
	[edit security nat] Hierarchy Level	64
	[edit security utm] Hierarchy Level	67
	[edit security idp] Hierarchy Level	74
	[edit security ike] Hierarchy Level	83
	[edit security ipsec] Hierarchy Level	85
	[edit security zones] Hierarchy Level	87
<b>Chapter 3</b>	<b>Administration</b>	<b>89</b>
	SRX Series Security	89
	Default UTM Policy for Branch SRX Series	89
	Default UTM Policy	89
	Predefined UTM Profile Configuration for Branch SRX Series	89
	Antispam	90
	Antivirus	90



Web Filtering .....	92
Operational Commands .....	96
request system license update .....	98
show security idp active-policy .....	99
show security idp status .....	100
show security flow session .....	102
show security nat destination summary .....	107
show security policies .....	109
show security utm session .....	116
show security utm status .....	117
show security zones .....	118
show system license (View) .....	121
show system services dhcp client .....	124

## Part 2

### Chapter 4

## Installation and Upgrade Guide for Security Devices

<b>Overview .....</b>	<b>129</b>
Product Overview .....	129
Junos OS Overview .....	129
One Operating System .....	129
One Software Release .....	130
One Modular Software Architecture .....	130
Junos OS Editions .....	130
Installation Categories on the J Series Services Routers .....	131
Software Naming Convention .....	131
Junos OS Release Numbers .....	132
Hardware Overview (J Series Services Routers) .....	134
System Memory .....	134
Storage Media .....	135
Software Installation and Upgrade .....	135
Installation Type Overview .....	136
Standard Installation .....	136
Category Change Installation .....	136
Recovery Installation .....	136
Software Package Information Security .....	137
Understanding Junos OS Upgrades for SRX Series Devices .....	137
Understanding Junos OS Upgrades for J Series Devices .....	138
Junos OS Upgrade Methods on the SRX Series Devices .....	138
Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices .....	139
Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices .....	140
Junos OS Upgrade Packages .....	140
Junos OS Recovery Packages .....	141
Installation Modules .....	142
Understanding Download Manager .....	143
Overview .....	143
Using Download Manager to Upgrade Junos OS .....	143
Handling Errors .....	144

Considerations . . . . .	144
Dual-Root Partitioning and Autorecovery . . . . .	145
Dual-Root Partitioning Scheme Overview . . . . .	145
Boot Media and Boot Partition on the SRX Series Devices . . . . .	146
Important Features of the Dual-Root Partitioning Scheme . . . . .	146
Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information . . . . .	147
Overview . . . . .	147
How Autorecovery Works . . . . .	147
How to Use Autorecovery . . . . .	148
Data That Is Backed Up in an Autorecovery . . . . .	148
Troubleshooting Alarms . . . . .	148
Considerations . . . . .	149
BIOS Upgrade . . . . .	149
Understanding Auto BIOS Upgrade Using Junos CLI . . . . .	149
Understanding Manual BIOS Upgrade Using Junos CLI . . . . .	150
Autoinstallation . . . . .	151
Autoinstallation Overview . . . . .	151
Automatic Installation of Configuration Files . . . . .	152
Supported Autoinstallation Interfaces and Protocols . . . . .	152
Typical Autoinstallation Process on a New Device . . . . .	153
Automatic Installation of Configuration Files (J Series Services Routers and SRX Series Services Gateways) . . . . .	154
J Series Automatic Installation Overview . . . . .	154
SRX Series Services Gateways Automatic Installation Overview . . . . .	156
Licenses . . . . .	156
Junos OS License Overview . . . . .	156
License Enforcement . . . . .	157
License Key Components . . . . .	157
License Management Fields Summary . . . . .	157
License Enforcement . . . . .	159
Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways . . . . .	159
<b>Chapter 5</b>	
<b>Installation . . . . .</b>	<b>163</b>
Software Installation and Upgrade . . . . .	163
Upgrading Individual Software Packages . . . . .	164
Preparing Your SRX Series Device for Junos OS Upgrades . . . . .	166
Preparing Your J Series Services Router for Junos OS Upgrades . . . . .	167
Preparing the USB Flash Drive to Upgrade Junos OS . . . . .	168
Determining the Junos OS Version . . . . .	170
Connecting to the Console Port . . . . .	170
Backing Up the Current Installation (J Series Services Routers and SRX Series Services Gateways) . . . . .	171
Downloading Software . . . . .	172
Downloading Software with a Browser . . . . .	172
Downloading Software Using the Command-Line Interface . . . . .	173
Downloading Junos OS Upgrades for SRX Series Devices . . . . .	174
Downloading Junos OS Upgrades for J Series Devices . . . . .	175

Checking the Current Configuration and Candidate Software	
Compatibility . . . . .	175
Verifying Available Disk Space on SRX Series Devices . . . . .	176
Example: Installing Junos OS Upgrades on SRX Series Devices . . . . .	177
Example: Installing Junos OS Upgrades on J Series Devices . . . . .	179
Installing Junos OS Using TFTP on SRX Series Devices . . . . .	181
Installing Junos OS Using a USB Flash Drive on SRX Series Devices . . . . .	184
Installing Junos OS Upgrades from a Remote Server on the SRX Series	
Devices . . . . .	185
Installing Junos OS Upgrades from a Remote Server on J Series Devices . .	186
Dual-Root Partitioning and Autorecovery . . . . .	187
Understanding Automatic Recovery of the Primary Junos OS Image with	
Dual-Root Partitioning . . . . .	188
Understanding How the Primary Junos OS Image with Dual-Root Partitioning	
Recovers on SRX Series Devices . . . . .	190
Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with	
Dual-Root Partitioning . . . . .	191
Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on	
SRX Series Devices . . . . .	192
Example: Installing Junos OS on SRX Series Devices Using the Partition	
Option . . . . .	193
Reinstalling the Single-Root Partition Using request system software add	
Command . . . . .	196
Boot Loaders and Boot Devices . . . . .	197
Installing Junos OS from the Boot Loader Using a USB Storage Device on	
an SRX Series Device . . . . .	197
Upgrading the Boot Loader on SRX Series Devices . . . . .	198
Software Downgrade . . . . .	199
Example: Downgrading Junos OS on SRX Series Devices . . . . .	199
Example: Downgrading Junos OS on J Series Devices . . . . .	201
<b>Chapter 6 Configuration . . . . .</b>	<b>205</b>
Autoinstallation . . . . .	205
Example: Configuring Autoinstallation . . . . .	205
Backup and Snapshot Configuration Files . . . . .	208
Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots	
in J Series Devices . . . . .	208
Configuring External CompactFlash on SRX650 Devices . . . . .	209
Boot Loaders and Boot Devices . . . . .	210
Example: Configuring Boot Devices for SRX Series Devices . . . . .	210
Example: Configuring Boot Devices for J Series Devices . . . . .	213
Configuration Statements . . . . .	215
System Configuration Statement Hierarchy . . . . .	215
autoinstallation . . . . .	246
configuration-servers . . . . .	247
interfaces (Autoinstallation) . . . . .	248
license . . . . .	249
usb . . . . .	251

<b>Chapter 7</b>	<b>Administration . . . . .</b>	<b>253</b>
	Auto BIOS . . . . .	253
	Disabling Auto BIOS Upgrade on SRX Series Devices . . . . .	253
	Licenses . . . . .	253
	Displaying License Keys . . . . .	254
	Generating a License Key . . . . .	254
	Downloading License Keys . . . . .	255
	Saving License Keys . . . . .	255
	Updating License Keys . . . . .	256
	Example: Adding a New License Key . . . . .	257
	Example: Deleting a License Key . . . . .	260
	Software Stop and Restart . . . . .	261
	Example: Rebooting SRX Series Devices . . . . .	262
	Example: Rebooting J Series Devices . . . . .	263
	Restarting the Chassis on SRX Series Devices . . . . .	265
	Restarting the Chassis on J Series Devices . . . . .	266
	Example: Halting SRX Series Devices . . . . .	266
	Example: Halting J Series Devices . . . . .	268
	Bringing Chassis Components Online and Offline on SRX Series Devices . . . . .	270
	Bringing Chassis Components Online and Offline on J Series Devices . . . . .	271
	Operational Commands . . . . .	271
	request system autorecovery state . . . . .	273
	request system download abort . . . . .	275
	request system download clear . . . . .	276
	request system download pause . . . . .	277
	request system download resume . . . . .	278
	request system download start . . . . .	279
	request system firmware upgrade . . . . .	280
	request system license update . . . . .	281
	request system partition compact-flash . . . . .	282
	request system power-off fpc . . . . .	283
	request system snapshot (Maintenance) . . . . .	284
	request system software abort in-service-upgrade (ICU) . . . . .	287
	request system software add (Maintenance) . . . . .	288
	request system reboot . . . . .	289
	request system software rollback (Maintenance) . . . . .	290
	show chassis usb storage . . . . .	291
	show system autorecovery state . . . . .	292
	show system auto-snapshot . . . . .	294
	show system download . . . . .	296
	show system license (View) . . . . .	298
	show system login logout . . . . .	301
	show system snapshot media . . . . .	302
	show system storage (View SRX Series) . . . . .	303
	show system storage partitions (View SRX Series) . . . . .	305
	show version . . . . .	306

<b>Part 3</b>	<b>CLI User Guide</b>	
<b>Chapter 8</b>	<b>Overview</b>	<b>309</b>
	CLI Overview	309
	Introducing the Junos OS Command-Line Interface	309
	Key Features of the CLI	310
	Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies	311
	Junos OS CLI Command Modes	311
	CLI Command Hierarchy	312
	Configuration Statement Hierarchy	312
	Moving Among Hierarchy Levels	313
	Other Tools to Configure and Monitor Devices Running Junos OS	314
	Commands and Configuration Statements for Junos-FIPS	314
	CLI Online Help	315
	Getting Online Help from the Junos OS Command-Line Interface	315
	Getting Help About Commands	315
	Getting Help About a String in a Statement or Command	316
	Getting Help About Configuration Statements	316
	Getting Help About System Log Messages	317
	Junos OS CLI Online Help Features	317
	Help for Omitted Statements	317
	Using CLI Command Completion	318
	Using Command Completion in Configuration Mode	318
	Displaying Tips About CLI Commands	318
	CLI Operational Mode	319
	Overview of Junos OS CLI Operational Mode Commands	319
	CLI Command Categories	319
	Commonly Used Operational Mode Commands	320
	Junos OS Operational Mode Commands That Combine Other Commands	322
	Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands	322
	Controlling the Scope of an Operational Mode Command	323
	Operational Mode Commands on a TX Matrix Router or TX Matrix Plus Router	324
	Examples of Routing Matrix Command Options	325
	Using the Pipe (   ) Symbol to Filter Junos Command Output	327
	Using Regular Expressions with the Pipe (   ) Symbol to Filter Junos Command Output	327
	Pipe (   ) Filter Functions in the Junos OS command-line interface	328
	Comparing Configurations	329
	Counting the Number of Lines of Output	330
	Displaying Output in XML Tag Format	330
	Displaying the RPC tags for a Command	331
	Ignoring Output That Does Not Match a Regular Expression	331
	Displaying Output from the First Match of a Regular Expression	331
	Retaining Output After the Last Screen	332
	Displaying Output Beginning with the Last Entries	332

Displaying Output That Matches a Regular Expression . . . . .	332
Preventing Output from Being Paginated . . . . .	333
Sending Command Output to Other Users . . . . .	333
Resolving IP Addresses . . . . .	333
Saving Output to a File . . . . .	334
Trimming Output by Specifying the Starting Column . . . . .	334
CLI Configuration Mode . . . . .	334
Understanding Junos OS CLI Configuration Mode . . . . .	334
Configuration Mode Commands . . . . .	336
Configuration Statements and Identifiers . . . . .	337
Configuration Statement Hierarchy . . . . .	339
Modifying the Junos OS Configuration . . . . .	341
Commit Operation When Multiple Users Configure the Software . . . . .	341
Forms of the configure Command . . . . .	342
Additional Details About Specifying Junos Statements and Identifiers . . . . .	344
Specifying Statements . . . . .	344
Performing CLI Type-Checking . . . . .	346
CLI Advanced Features . . . . .	347
Using Keyboard Sequences to Move Around and Edit the Junos OS CLI . . . . .	347
Using Wildcard Characters in Interface Names . . . . .	349
Using Global Replace in a Junos Configuration . . . . .	349
CLI Commit Operations . . . . .	350
Junos OS Commit Model for Router or Switch Configuration . . . . .	350
Commit Operation When Multiple Users Configure the Software . . . . .	351
Junos OS Batch Commits Overview . . . . .	352
Aggregation and Error Handling . . . . .	352
Configuration Groups . . . . .	353
Understanding the Junos Configuration Groups . . . . .	353
Configuration Groups Overview . . . . .	353
Inheritance Model . . . . .	354
Configuring Configuration Groups . . . . .	354
Configuration Management . . . . .	354
Understanding How the Junos Configuration Is Stored . . . . .	354
<b>Chapter 9 Configuration . . . . .</b>	<b>357</b>
Getting Started with Junos OS Configuration . . . . .	357
Entering and Exiting the Junos OS CLI Configuration Mode . . . . .	358
Displaying the Current Junos OS Configuration . . . . .	360
Example: Displaying the Current Junos OS Configuration . . . . .	360
Displaying set Commands from the Junos OS Configuration . . . . .	361
Example: Displaying set Commands from the Configuration . . . . .	362
Example: Displaying Required set Commands at the	
Current Hierarchy Level . . . . .	362
Example: Displaying set Commands with the match Option . . . . .	363
Displaying Users Currently Editing the Configuration . . . . .	364
Displaying Additional Information About the Configuration . . . . .	364
Using the configure exclusive Command . . . . .	367
Updating the configure private Configuration . . . . .	368
Getting Started with the Junos OS Command-Line Interface . . . . .	368

Switching Between Junos OS CLI Operational and Configuration Modes . .	370
Configuring a User Account on a Device Running Junos OS . . . . .	372
Example: Configuring a Routing Protocol . . . . .	374
Shortcut . . . . .	375
Longer Configuration . . . . .	375
Making Changes to a Routing Protocol Configuration . . . . .	377
Updating the Junos OS Configuration . . . . .	380
Adding Junos Configuration Statements and Identifiers . . . . .	380
Deleting a Statement from a Junos Configuration . . . . .	382
Example: Deleting a Statement from the Junos Configuration . . . . .	383
Copying a Junos Statement in the Configuration . . . . .	384
Example: Copying a Statement in the Junos Configuration . . . . .	384
Issuing Relative Junos Configuration Mode Commands . . . . .	385
Renaming an Identifier in a Junos Configuration . . . . .	385
Example: Renaming an Identifier in a Junos Configuration . . . . .	386
Inserting a New Identifier in a Junos Configuration . . . . .	386
Example: Inserting a New Identifier in a Junos Configuration . . . . .	386
Deactivating and Reactivating Statements and Identifiers in a Junos Configuration . . . . .	388
Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration . . . . .	389
Adding Comments in a Junos Configuration . . . . .	390
Example: Including Comments in a Junos Configuration . . . . .	391
Using Regular Expressions to Delete Related Items from a Junos Configuration . . . . .	393
Example: Using the Wildcard Command with the Range Option . . . . .	394
Committing a Junos OS Configuration . . . . .	398
Verifying a Junos Configuration . . . . .	399
Example: Protecting the Junos OS Configuration from Modification or Deletion . . . . .	399
Committing a Junos OS Configuration . . . . .	406
Committing a Junos Configuration and Exiting Configuration Mode . . . . .	408
Activating a Junos Configuration but Requiring Confirmation . . . . .	409
Scheduling a Junos Commit Operation . . . . .	410
Monitoring the Junos Commit Process . . . . .	411
Adding a Comment to Describe the Committed Configuration . . . . .	412
Backing Up the Committed Configuration on the Alternate Boot Drive . . . .	413
Example: Configuring Junos OS Batch Commits . . . . .	414
Junos OS Batch Commits Overview . . . . .	414
Example: Configuring Batch Commit Server Properties . . . . .	414
Loading a Junos OS Configuration . . . . .	421
Loading a Configuration from a File . . . . .	421
Examples: Loading a Configuration from a File . . . . .	424
Synchronizing the Junos OS Configuration . . . . .	426
Synchronizing Routing Engines . . . . .	426

Creating and Applying Junos OS Configuration Groups . . . . .	427
Creating a Junos Configuration Group . . . . .	428
Applying a Junos Configuration Group . . . . .	429
Example: Configuring and Applying Junos Configuration Groups . . . . .	431
Example: Creating and Applying Configuration Groups on a TX Matrix Router . . . . .	432
Disabling Inheritance of a Junos OS Configuration Group . . . . .	433
Using Wildcards with Configuration Groups . . . . .	435
Example: Using Conditions to Apply Configuration Groups . . . . .	438
Using Conditions to Apply Configuration Groups Overview . . . . .	438
Example: Configuring Conditions for Applying Configuration Groups . .	438
Example : Configuring Sets of Statements with Configuration Groups . . .	440
Example: Configuring Interfaces Using Junos OS Configuration Groups . .	442
Example: Configuring a Consistent IP Address for the Management Interface . . . . .	444
Example: Configuring Peer Entities . . . . .	445
Establishing Regional Configurations . . . . .	447
Selecting Wildcard Names . . . . .	448
Using Junos OS Defaults Groups . . . . .	450
Example: Referencing the Preset Statement From the Junos defaults Group . . . . .	451
Example: Viewing Default Statements That Have Been Applied to the Configuration . . . . .	452
CLI Online Help . . . . .	452
Examples: Using Command Completion in Configuration Mode . . . . .	452
Examples: Using the Junos OS CLI Command Completion . . . . .	454
Displaying the Junos OS CLI Command and Word History . . . . .	455
CLI Configuration Mode . . . . .	455
Example: Using the configure Command . . . . .	455
Controlling the CLI Environment . . . . .	456
Example: Controlling the CLI Environment . . . . .	456
CLI Advanced Features . . . . .	456
Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference . . . . .	456
Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name . . . . .	457
Example: Using Global Replace in a Junos Configuration—Using the upto Option . . . . .	458
Configuration Statements . . . . .	460
apply-groups . . . . .	461
apply-groups-except . . . . .	461
commit-interval (Batch Commits) . . . . .	462
groups . . . . .	463
days-to-keep-error-logs (Batch Commits) . . . . .	465
deactivate . . . . .	466
delete . . . . .	467
edit . . . . .	468
exit . . . . .	469
help . . . . .	470



	insert .....	471
	load .....	472
	maximum-aggregate-pool (Batch Commits) .....	473
	maximum-entries (Batch Commits) .....	474
	protect .....	475
	quit .....	476
	rename .....	477
	rename .....	478
	replace .....	479
	rollback .....	480
	run .....	481
	save .....	482
	server (Batch Commits) .....	483
	set .....	484
	status .....	485
	top .....	486
	traceoptions (Batch Commits) .....	487
	unprotect .....	488
	up .....	489
	update .....	490
	when .....	491
	wildcard delete .....	492
<b>Chapter 10</b>	<b>Administration .....</b>	<b>493</b>
	CLI Operational Mode .....	493
	Interface Naming Conventions Used in the Junos OS Operational	
	Commands .....	493
	Physical Part of an Interface Name .....	493
	Logical Part of an Interface Name .....	494
	Channel Identifier Part of an Interface Name .....	494
	Routine Monitoring .....	495
	Checking the Status of a Device Running Junos OS .....	495
	Monitoring Who Uses the Junos OS CLI .....	497
	Viewing Files and Directories on a Device Running Junos OS .....	497
	Directories on the Router or Switch .....	498
	Listing Files and Directories .....	498
	Specifying Filenames and URLs .....	500
	Displaying Junos OS Information .....	501
	Managing Programs and Processes Using Junos OS Operational Mode	
	Commands .....	503
	Showing Software Processes .....	504
	Restarting a Junos OS Process .....	505
	Stopping the Junos OS .....	506
	Rebooting the Junos OS .....	507
	Using the Junos OS CLI Comment Character # for Operational Mode	
	Commands .....	508
	Example: Using Comments in Junos OS Operational Mode Commands ..	508

Managing the CLI Environment .....	509
Controlling the Junos OS CLI Environment .....	509
Setting the Terminal Type .....	510
Setting the CLI Prompt .....	510
Setting the CLI Directory .....	510
Setting the CLI Timestamp .....	510
Setting the Idle Timeout .....	511
Setting the CLI to Prompt After a Software Upgrade .....	511
Setting Command Completion .....	511
Displaying CLI Settings .....	511
Overview of Junos OS CLI Operational Mode Commands .....	512
CLI Command Categories .....	512
Commonly Used Operational Mode Commands .....	513
Setting the Junos OS CLI Screen Length and Width .....	514
Setting the Screen Length .....	514
Setting the Screen Width .....	515
Understanding the Screen Length and Width Settings .....	515
CLI Advanced Features .....	515
Common Regular Expressions to Use with the replace Command .....	516
Junos OS CLI Environment Commands .....	517
set cli complete-on-space .....	518
set cli directory .....	519
set cli idle-timeout .....	520
set cli prompt .....	521
set cli restart-on-upgrade .....	522
set cli screen-length .....	523
set cli screen-width .....	524
set cli terminal .....	525
set cli timestamp .....	526
set date .....	527
show cli .....	528
show cli authorization .....	530
show cli directory .....	531
show cli history .....	532
Operational Commands .....	532
(pipe) .....	533
activate .....	535
annotate .....	536
commit .....	537
configure .....	540
copy .....	542
file .....	543
help .....	544
request .....	545
restart .....	547
set .....	557
show .....	558
show configuration .....	559
show   display inheritance .....	562

	show   display omit . . . . .	563
	show   display set . . . . .	564
	show   display set relative . . . . .	565
	show groups junos-defaults . . . . .	566
	show system commit . . . . .	567
<b>Chapter 11</b>	<b>Troubleshooting . . . . .</b>	<b>569</b>
	Troubleshooting Procedures . . . . .	569
	Returning to the Most Recently Committed Junos Configuration . . . . .	569
	Returning to a Previously Committed Junos OS Configuration . . . . .	569
	Returning to a Configuration Prior to the One Most Recently Committed . . . . .	570
	Displaying Previous Configurations . . . . .	570
	Comparing Configuration Changes with a Prior Version . . . . .	571
	Creating and Returning to a Rescue Configuration . . . . .	573
	Saving a Configuration to a File . . . . .	573
	Creating and Returning to a Rescue Configuration . . . . .	574
	Rolling Back Junos OS Configuration Changes . . . . .	575
<b>Part 4</b>	<b>J-Web User Guide</b>	
<b>Chapter 12</b>	<b>Overview . . . . .</b>	<b>579</b>
	J-Web User Interface . . . . .	579
	J-Web Overview . . . . .	579
	J-Web Layout . . . . .	580
	Top Pane Elements . . . . .	580
	Main Pane Elements . . . . .	581
	Side Pane Elements . . . . .	582
	Navigating the J-Web Interface . . . . .	583
	Navigating the J-Web Configuration Editor . . . . .	584
	Getting J-Web Help . . . . .	584
	Installation and Setup . . . . .	585
	J-Web Software Requirements . . . . .	585
	Installing the J-Web Software . . . . .	585
	Starting the J-Web Interface . . . . .	586
	Configuring Basic Settings . . . . .	588
	Secure Web Access . . . . .	591
	Secure Web Access Overview . . . . .	591
	Generating SSL Certificates . . . . .	592
<b>Chapter 13</b>	<b>Configuration . . . . .</b>	<b>593</b>
	Configuration Tools . . . . .	593
	Configuration Task Overview . . . . .	593
	Point and Click CLI (J-Web Configuration Editor) . . . . .	595
	CLI Viewer (View Configuration Text) . . . . .	597
	CLI Editor (Edit Configuration Text) . . . . .	599
	CLI Terminal Requirements . . . . .	600
	Starting the CLI Terminal . . . . .	600

	Using the CLI Terminal .....	601
	Configuration Tasks .....	603
	Editing and Committing a Junos OS Configuration .....	603
	J-Web Configuration Tasks .....	604
	Editing a Configuration .....	604
	Committing a Configuration .....	607
	Discarding Parts of a Candidate Configuration .....	607
	Accounting Options .....	608
<b>Chapter 14</b>	<b>Administration .....</b>	<b>611</b>
	Session and User Management .....	611
	Setting J-Web Session Limits .....	611
	Terminating J-Web Sessions .....	612
	Viewing Current Users .....	612
	Secure Web Access .....	612
	Configuring Secure Web Access .....	612
	Alarms .....	615
	Using Alarms .....	615
	View Alarms .....	615
	Active Alarms Information .....	616
	Alarm Severity .....	616
	Displaying Alarm Descriptions .....	616
	Sample Task—Viewing and Filtering Alarms .....	616
	Events .....	617
	Using View Events .....	617
	Viewing Events .....	618
	View Events .....	618
	Understanding Severity Levels .....	619
	Using Filters .....	619
	Using Regular Expressions .....	621
	Sample Task—Filtering and Viewing Events .....	622
	Device Management .....	623
	Using Software (J Series Routing Platforms Only) .....	623
	Using Licenses (J Series Routing Platform Only) .....	624
	Using Snapshot (J Series Routing Platforms Only) .....	625
	Sample Task—Manage Snapshots .....	626
	Using Reboot .....	627
	Monitoring in J-Web .....	627
	Monitor Task Overview .....	628
	Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only) .....	628
	Class of Service .....	629
	Interfaces .....	630
	MPLS .....	631
	PPPoE (J Series Routing Platforms Only) .....	632
	RPM .....	632

	Routing .....	633
	Security .....	634
	Firewall .....	634
	IPsec .....	635
	NAT .....	635
	Service Sets .....	636
	Services .....	636
	System View .....	636
	System Information .....	637
	Chassis Information .....	637
	Process Details .....	637
	FEB Redundancy (M120 Routing Platforms Only) .....	638
	Sample Task—Monitoring Interfaces .....	638
	Sample Task—Monitoring Route Information .....	640
	Configuration and File Management .....	642
	Displaying Configuration History .....	642
	Displaying Users Editing the Configuration .....	644
	Loading a Previous Configuration File .....	645
	Downloading a Configuration File .....	646
	Comparing Configuration Files .....	646
	Upload Configuration File .....	647
	Using Rescue (J Series Routing Platforms Only) .....	648
	Using Files .....	648
<b>Chapter 15</b>	<b>Troubleshooting .....</b>	<b>651</b>
	J-Web User Interface .....	651
	Lost Router Connectivity .....	651
	Unpredictable J-Web Behavior .....	651
	No J-Web Access .....	652
	Events .....	652
	Troubleshooting Events .....	652
	Network .....	653
	Using Ping Host .....	653
	Using Ping MPLS .....	654
	Using Ping ATM (M Series, MX Series, and T Series Routing Platforms Only) .....	656
	Using Traceroute .....	656
	Using Packet Capture .....	656
	Sample Task—Ping Host .....	657

## Part 5

## Administration Library for Security Devices

## Chapter 16

## Administration Guide for Security Devices ..... 663

Overview .....	663
Secure Web Access .....	663
Secure Web Access Overview .....	663
J-Web User Interface .....	664
Understanding the User Interfaces .....	664
Starting the J-Web User Interface .....	666
Understanding the J-Web Interface Layout .....	667
J-Web Commit Options Guidelines .....	669
Getting Help in the J-Web User Interface .....	670
Establishing J-Web Sessions .....	671
User Authentication and Access .....	671
Understanding User Authentication Methods .....	671
Understanding User Accounts .....	672
Understanding Login Classes .....	673
Understanding Template Accounts .....	676
USB Modems for Remote Management Setup .....	676
USB Modem Interface Overview .....	676
USB Modem Configuration Overview .....	679
Telnet and SSH Device Control .....	681
Securing the Console Port Configuration Overview .....	681
Reverse Telnet Overview .....	683
DHCP for IP Address Device .....	684
DHCP Server, Client, and Relay Agent Overview .....	684
DHCP Configuration Overview .....	685
Understanding DHCP Server Operation .....	686
Understanding DHCP Client Operation .....	687
Understanding DHCP Relay Agent Operation .....	687
DHCP Settings and Restrictions Overview .....	688
Understanding DHCP Services in a Routing Instance .....	689
DHCPv6 Client .....	692
DHCPv6 Client Overview .....	693
Understanding DHCPv6 Client and Server Identification .....	693
DHCPv6 Local Server .....	694
DHCPv6 Server Overview .....	694
File Management .....	695
File Management Overview .....	695
Licenses .....	695
Junos OS License Overview .....	696
Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways .....	698
Configuration .....	699
USB Modems for Remote Management Setup .....	699
Example: Configuring a USB Modem Interface .....	699
Example: Configuring a Dialer Interface .....	702

Example: Configuring a Dialer Interface for USB Modem Dial-In . . . . .	705
Configuring a Dial-Up Modem Connection Remotely . . . . .	707
DHCP for IP Address Device . . . . .	708
Example: Configuring the Device as a DHCP Server . . . . .	709
Example: Configuring the Device as a DHCP Client . . . . .	714
Example: Configuring the Device as a BOOTP or DHCP Relay Agent . . . . .	718
Configuring a DHCP Local Server . . . . .	723
Configuring a DHCP Client . . . . .	727
Configuring a DHCP Relay Agent . . . . .	729
Minimum DHCP Local Server Configuration . . . . .	730
Configuring Address-Assignment Pools . . . . .	731
Configuring an Address-Assignment Pool Name and Addresses . . . . .	731
Configuring DHCP Client-Specific Attributes . . . . .	732
Configuring a Named Address Range for Dynamic Address Assignment . . . . .	732
Configuring Static Address Assignments . . . . .	733
Enabling TCP/IP Propagation on a DHCP Local Server . . . . .	734
Minimum DHCP Client Configuration . . . . .	734
Configuring Optional DHCP Client Attributes . . . . .	735
Minimum DHCP Relay Agent Configuration . . . . .	736
DHCPv6 Client . . . . .	736
Minimum DHCPv6 Client Configuration . . . . .	736
Configuring Optional DHCPv6 Client Attributes . . . . .	737
Configuring Nontemporary Address Assignment . . . . .	738
Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation . . . . .	739
Configuring Auto-Prefix Delegation . . . . .	739
Configuring the DHCPv6 Client Rapid Commit Option . . . . .	740
Configuring a DHCPv6 Client in Autoconfig Mode . . . . .	741
Configuring TCP/IP Propagation on a DHCPv6 Client . . . . .	741
DHCPv6 Local Server . . . . .	742
Creating a Security Policy for DHCPv6 . . . . .	742
Example: Configuring DHCPv6 Server Options . . . . .	743
Example: Configuring an Address-Assignment Pool . . . . .	745
Configuring a Named Address Range for Dynamic Address Assignment . . . . .	748
Configuring Address-Assignment Pool Linking . . . . .	748
Configuring DHCP Client-Specific Attributes . . . . .	749
Configuring an Address-Assignment Pool for Router Advertisement . . . . .	750
Configuration Statements . . . . .	750
[edit security certificates] Hierarchy Level . . . . .	752
[edit security ssh-known-hosts] Hierarchy Level . . . . .	752
Interfaces Configuration Statement Hierarchy . . . . .	753
Groups Configuration Statement Hierarchy . . . . .	768
address-assignment (Access) . . . . .	769
address-pool (Access) . . . . .	772
allow-configuration . . . . .	773
allow-configuration-regexps . . . . .	774
authentication-key . . . . .	775

authentication-order	776
boot-server (NTP)	777
broadcast	778
broadcast-client	779
client-ia-type	779
client-identifier (dhcp-client)	780
client-identifier (dhcpv6-client)	780
client-list-name (SNMP)	781
client-type	781
deny-configuration	782
deny-configuration-regexps	783
dhcp-attributes (Access IPv4 Address Pools)	784
dhcp-attributes (Access IPv6 Address Pools)	786
dhcp-client	787
dhcpv6-client	788
dhcp-local-server (System Services)	789
dhcpv6 (System Services)	793
family (Security Forwarding Options)	797
forwarding-options (Security)	798
group (System Services DHCP)	799
host (SSH Known Hosts)	802
hostkey-algorithm	803
interface (System Services DHCP)	804
interfaces (ARP)	805
interfaces (Security Zones)	806
interface-traceoptions (System Services DHCP)	807
internet-options	809
lease-time (dhcp-client)	810
lockout-period	811
multicast-client	811
name-server (Access)	812
neighbor-discovery-router-advertisement (Access)	812
ntp	813
overrides (System Services DHCP)	814
peer (NTP)	815
port (System Services Reverse SSH)	816
port (System Services Reverse Telnet)	816
prefix	817
proflerd	818
proxy	819
rapid-commit	819
reconfigure (System Services DHCP)	820
req-option	821
retransmission-attempt (dhcp-client)	822
retransmission-attempt (dhcpv6-client)	822
retransmission-interval (dhcp-client)	823
ssh (reverse)	823
ssh-known-hosts	824
server (NTP)	825



server-address (dhcp-client) . . . . .	826
services . . . . .	827
source-address (NTP, RADIUS, System Logging, or TACACS+) . . . . .	832
telnet (System Services Reverse) . . . . .	832
traceoptions (System Services DHCP) . . . . .	833
trusted-key . . . . .	835
update-router-advertisement . . . . .	835
update-server (dhcp-client) . . . . .	836
update-server (dhcpv6-client) . . . . .	836
user-id . . . . .	836
use-interface . . . . .	837
vendor-id . . . . .	837
vpn (Forwarding Options) . . . . .	838
Configuration Statements (System) . . . . .	838
System Configuration Statement Hierarchy . . . . .	839
ciphers . . . . .	870
connection-limit . . . . .	871
disable (System Services) . . . . .	872
dlv . . . . .	872
kernel-replication (System) . . . . .	873
location . . . . .	874
macs . . . . .	875
protocol-version . . . . .	876
radius-server . . . . .	877
root-authentication . . . . .	878
single-connection . . . . .	879
static-subscribers . . . . .	879
statistics-service . . . . .	880
subscriber-management . . . . .	880
subscriber-management-helper . . . . .	881
uac-service . . . . .	882
usb-control . . . . .	883
watchdog . . . . .	883
web-management . . . . .	884
web-management (System Services) . . . . .	885
Administration . . . . .	888
Secure Web Access . . . . .	888
Generating an SSL Certificate Using the openssl Command . . . . .	888
Generating a Self-Signed SSL Certificate . . . . .	889
Manually Generating Self-Signed SSL Certificates . . . . .	889
Configuring Device Addresses . . . . .	890
Enabling Access Services . . . . .	891
Example: Configuring Secure Web Access . . . . .	892
Adding, Editing, and Deleting Certificates on the Device . . . . .	894
User Authentication and Access . . . . .	894
Example: Configuring a RADIUS Server for System Authentication . . . . .	895
Example: Configuring a TACACS+ Server for System Authentication . . . . .	897
Example: Configuring Authentication Order . . . . .	900

Example: Configuring New Users .....	902
Example: Configuring System Retry Options .....	905
Example: Creating Template Accounts .....	908
Handling Authorization Failure .....	911
Understanding Administrative Roles .....	912
Example: Configuring Administrative Roles .....	914
USB Modems for Remote Management Setup .....	921
Connecting to the Device Remotely .....	921
Modifying USB Modem Initialization Commands .....	921
Resetting USB Modems .....	922
Telnet and SSH Device Control .....	922
Configuring Password Retry Limits for Telnet and SSH Access .....	923
Configuring Reverse Telnet and Reverse SSH .....	924
Example: Controlling Management Access on SRX and J-Series Devices .....	925
The telnet Command .....	928
The ssh Command .....	929
DHCP for IP Address Device .....	930
Verifying and Managing DHCP Local Server Configuration .....	930
Verifying and Managing DHCP Client Configuration .....	930
Verifying and Managing DHCP Relay Configuration .....	931
File Management .....	932
Decrypting Configuration Files .....	932
Encrypting Configuration Files .....	932
Modifying the Encryption Key .....	934
Cleaning Up Files .....	934
Cleaning Up Files with the CLI .....	935
Deleting Files .....	936
Deleting the Backup Software Image .....	937
Downloading Files .....	937
Managing Accounting Files .....	938
Licenses .....	938
Displaying License Keys .....	938
Downloading License Keys .....	939
Generating a License Key .....	939
Saving License Keys .....	940
Updating License Keys .....	941
Example: Adding a New License Key .....	941
Example: Deleting a License Key .....	945
Operational Commands .....	946
clear dhcp client binding .....	949
clear dhcpv6 client binding .....	950
clear dhcp client statistics .....	951
clear dhcpv6 client statistics .....	952
clear dhcp relay binding .....	953
clear dhcp relay statistics .....	954
clear dhcp server binding .....	955
clear dhcp server statistics .....	956
clear dhcpv6 server binding (Local Server) .....	957

clear dhcpv6 server statistics (Local Server) . . . . .	958
clear system login lockout . . . . .	959
file archive . . . . .	960
file checksum md5 . . . . .	962
file checksum sha1 . . . . .	963
file checksum sha-256 . . . . .	964
file compare . . . . .	965
file copy . . . . .	968
file delete . . . . .	970
file list . . . . .	971
file rename . . . . .	972
file show . . . . .	973
request dhcp client renew . . . . .	974
request dhcpv6 client renew . . . . .	975
request system autorecovery state . . . . .	976
request system download abort . . . . .	978
request system download clear . . . . .	979
request system download pause . . . . .	980
request system download resume . . . . .	981
request system download start . . . . .	982
request system firmware upgrade . . . . .	983
request system license update . . . . .	984
request system partition compact-flash . . . . .	985
request system power-off fpc . . . . .	986
request system services dhcp . . . . .	987
request system snapshot (Maintenance) . . . . .	988
request system software abort in-service-upgrade (ICU) . . . . .	991
request system software add (Maintenance) . . . . .	992
request system reboot . . . . .	993
request system software rollback (Maintenance) . . . . .	994
request support information . . . . .	995
request system zeroize . . . . .	1004
restart (Reset) . . . . .	1006
Restart Commands Overview . . . . .	1011
show chassis routing-engine (View) . . . . .	1012
show dhcp client binding . . . . .	1014
show dhcpv6 client binding . . . . .	1017
show dhcp client statistics . . . . .	1019
show dhcpv6 client statistics . . . . .	1021
show dhcp relay binding . . . . .	1023
show dhcp relay statistics . . . . .	1025
show dhcp server binding . . . . .	1027
show dhcp server statistics . . . . .	1029
show dhcpv6 server binding (View) . . . . .	1031
show dhcpv6 server statistics (View) . . . . .	1035
show firewall (View) . . . . .	1038
show system autorecovery state . . . . .	1040
show system directory-usage . . . . .	1042
show system download . . . . .	1044

	show system license (View) . . . . .	1046
	show system login lockout . . . . .	1049
	show system services dhcp client . . . . .	1050
	show system services dhcp relay-statistics . . . . .	1053
	show system snapshot media . . . . .	1055
	show system storage (View SRX Series) . . . . .	1056
	show system storage partitions (View SRX Series) . . . . .	1058
<b>Chapter 17</b>	<b>Access Privilege Administration Guide . . . . .</b>	<b>1059</b>
	Overview . . . . .	1059
	Introduction to Access Privileges . . . . .	1059
	Understanding Junos OS Access Privilege Levels . . . . .	1059
	Junos OS Login Classes Overview . . . . .	1063
	Access Privilege User Permission Flags Overview . . . . .	1064
	Specifying Access Privileges for Junos OS Configuration Mode	
	Hierarchies . . . . .	1066
	Configuration . . . . .	1067
	Configuring Access Privileges . . . . .	1067
	Configuring Access Privilege Levels . . . . .	1067
	Specifying Access Privileges for Junos OS Operational Mode	
	Commands . . . . .	1067
	Specifying Access Privileges for Junos OS Configuration Mode	
	Hierarchies . . . . .	1069
	Examples . . . . .	1069
	Example: Configuring Access Privilege Levels . . . . .	1070
	Example: Specifying Access Privileges Using	
	allow/deny-configuration-regexps Statements . . . . .	1070
	Example: Configuring Access Privileges for Operational Mode	
	Commands . . . . .	1074
	Example: Specifying Access Privileges Using	
	allow/deny-configuration-regexps Statements . . . . .	1075
	User Permission Flags Reference . . . . .	1078
	access . . . . .	1079
	access-control . . . . .	1080
	admin . . . . .	1081
	admin-control . . . . .	1082
	all-control . . . . .	1082
	clear . . . . .	1083
	configure . . . . .	1116
	control . . . . .	1116
	field . . . . .	1117
	firewall . . . . .	1117
	firewall-control . . . . .	1118
	floppy . . . . .	1119
	flow-tap . . . . .	1119
	flow-tap-control . . . . .	1119
	flow-tap-operation . . . . .	1120
	idp-profiler-operation . . . . .	1120
	interface . . . . .	1120

interface-control	1121
maintenance	1122
network	1128
pgcp-session-mirroring	1130
pgcp-session-mirroring-control	1130
reset	1131
rollback	1131
routing	1132
routing-control	1136
secret	1140
secret-control	1141
security	1142
security-control	1145
shell	1149
snmp	1149
system	1149
system-control	1151
trace	1153
trace-control	1158
view	1163
view-configuration	1225
Administration	1226
Operational Mode Commands	1226
show cli authorization	1227

## Part 6

### Chapter 18

## Monitoring and Troubleshooting Library for Security Devices

### Network Monitoring and Troubleshooting Guide for Security Devices . . . 1231

Overview	1231
Monitoring and Troubleshooting	1231
Monitoring Overview	1231
Diagnostic Tools Overview	1232
Accounting, Source Class Usage, and Destination Class Usage Options . .	1235
Accounting Options Overview	1235
Understanding Source Class Usage and Destination Class Usage Options	1236
Alarms	1237
Alarm Overview	1237
Data Path Debugging and Trace Options	1242
Understanding Data Path Debugging for SRX Series Devices	1242
Understanding Security Debugging Using Trace Options	1243
Understanding Flow Debugging Using Trace Options	1243
MPLS	1244
MPLS Connection Checking Overview	1244
Packet Capture	1246
Packet Capture Overview	1246

RPM .....	1248
RPM Overview .....	1248
RPM Support for VPN Routing and Forwarding .....	1252
Configuration .....	1253
Accounting, Source Class Usage, and Destination Class Usage Options ..	1253
Configuration Statements at the [edit accounting-options] Hierarchy	
Level .....	1253
Accounting Options Configuration .....	1254
Configuring Accounting-Data Log Files .....	1257
Configuring the Interface Profile .....	1260
Configuring the Filter Profile .....	1263
Example: Configuring a Filter Profile .....	1265
Example: Configuring Interface-Specific Firewall Counters	
and Filter Profiles .....	1265
Configuring SCU or DCU .....	1267
Configuring SCU on a Virtual Loopback Tunnel Interface .....	1269
Configuring Class Usage Profiles .....	1270
Configuring the MIB Profile .....	1272
Configuring the Routing Engine Profile .....	1274
Alarms .....	1276
Example: Configuring Interface Alarms .....	1276
Data Path Debugging and Trace Options .....	1278
Debugging the Data Path (CLI Procedure) .....	1279
Setting Security Trace Options (CLI Procedure) .....	1279
Setting Flow Debugging Trace Options (CLI Procedure) .....	1281
MPLS .....	1281
Configuring Ping MPLS .....	1281
Packet Capture .....	1282
Example: Enabling Packet Capture on a Device .....	1282
Example: Configuring Packet Capture on an Interface .....	1286
Example: Configuring a Firewall Filter for Packet Capture .....	1287
Example: Configuring Packet Capture for Datapath Debugging .....	1289
Disabling Packet Capture .....	1292
Deleting Packet Capture Files .....	1292
Changing Encapsulation on Interfaces with Packet Capture	
Configured .....	1293
RPM .....	1294
Example: Configuring Basic RPM Probes .....	1294
Example: Configuring RPM Using TCP and UDP Probes .....	1298
Example: Configuring RPM Probes for BGP Monitoring .....	1301
Directing RPM Probes to Select BGP Devices .....	1303
Configuring RPM Timestamping .....	1304
Tuning RPM Probes .....	1305
RPM Configuration Options .....	1306
Configuration Statements .....	1310
Configuration Statements at the [edit accounting-options] Hierarchy	
Level .....	1311
[edit security alarms] Hierarchy Level .....	1312
[edit security datapath-debug] Hierarchy Level .....	1313

[edit security traceoptions] Hierarchy Level .....	1314
accounting-options .....	1315
action-profile .....	1316
archive-sites .....	1317
capture-file (Security) .....	1318
class-usage-profile .....	1319
counters .....	1320
datapath-debug .....	1321
decryption-failures .....	1322
destination-classes .....	1323
destination-interface .....	1324
destination-port .....	1325
fields (for Interface Profiles) .....	1326
fields (for Routing Engine Profiles) .....	1327
file (Associating with a Profile) .....	1328
file (Configuring a Log File) .....	1329
files .....	1330
filter-profile .....	1330
flow (Security Flow) .....	1331
hardware-timestamp .....	1333
idp (Security Alarms) .....	1333
interface-profile .....	1334
interval .....	1335
maximum-capture-size (Datapath Debug) .....	1336
mib-profile .....	1336
mpls (Security Forwarding Options) .....	1337
next-hop .....	1337
nonpersistent .....	1338
object-names .....	1338
operation .....	1339
packet-capture .....	1340
packet-filter .....	1341
probe .....	1342
probe-interval .....	1343
probe-limit .....	1343
probe-server .....	1344
probe-type .....	1345
routing-engine-profile .....	1346
rpm (Services) .....	1347
size .....	1349
source-classes .....	1349
start-time .....	1350
target .....	1350
thresholds .....	1351
traceoptions (Security Datapath Debug) .....	1352
transfer-interval .....	1353
traps .....	1354

Administration .....	1354
Monitoring Security Devices .....	1355
Displaying Multicast Path Information .....	1356
Displaying Real-Time Interface Information .....	1358
Displaying Real-Time Monitoring Information .....	1360
Monitoring Address Pools .....	1362
Monitoring Antivirus Scan Engine Status .....	1363
Monitoring Antivirus Scan Results .....	1364
Monitoring Antivirus Session Status .....	1366
Monitoring Class-of-Service Performance .....	1367
Monitoring Content Filtering Configurations .....	1374
Monitoring CoS Classifiers .....	1375
Monitoring DHCP Client Bindings .....	1376
Monitoring Ethernet Switching .....	1377
Monitoring Events .....	1378
Monitoring GVRP .....	1380
Monitoring H.323 ALG Information .....	1381
Monitoring Interfaces .....	1382
Monitoring MGCP ALGs .....	1384
Monitoring MPLS Traffic Engineering Information .....	1387
Monitoring NAT .....	1392
Monitoring Policy Statistics .....	1402
Monitoring PPP .....	1403
Monitoring PPPoE .....	1404
Monitoring Reports .....	1407
Monitoring Routing Information .....	1413
Monitoring SCCP ALGs .....	1421
Monitoring Security Events by Policy .....	1423
Monitoring Security Features .....	1425
Monitoring SIP ALGs .....	1439
Monitoring Spanning Tree .....	1443
Monitoring the System .....	1444
Monitoring Voice ALG H.323 .....	1452
Monitoring Voice ALG MGCP .....	1454
Monitoring Voice ALG SCCP .....	1457
Monitoring Voice ALG SIP .....	1460
Monitoring Voice ALG Summary .....	1465
Monitoring VPNs .....	1466
Monitoring the WAN Acceleration Interface .....	1476
Monitoring Web Filtering Configurations .....	1476
Alarms .....	1477
Monitoring Active Alarms on a Device .....	1477
Monitoring Alarms .....	1478
Data Path Debugging and Trace Options .....	1479
Displaying a List of Devices .....	1480
Displaying Log and Trace Files .....	1481
Displaying Output for Security Trace Options .....	1481
Displaying Multicast Trace Operations .....	1482



Using the J-Web Traceroute Tool .....	1483
J-Web Traceroute Results and Output Summary .....	1484
MPLS .....	1485
Using the ping Command .....	1486
Using the J-Web Ping Host Tool .....	1488
J-Web Ping Host Results and Output Summary .....	1490
Using the J-Web Ping MPLS Tool .....	1491
J-Web Ping MPLS Results and Output Summary .....	1494
Pinging Layer 2 Circuits .....	1494
Pinging Layer 2 VPNs .....	1495
Pinging Layer 3 VPNs .....	1497
Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs .....	1498
Packet Capture .....	1499
Displaying Packet Headers .....	1499
Using the J-Web Packet Capture Tool .....	1503
J-Web Packet Capture Results and Output Summary .....	1506
RPM .....	1507
Monitoring RPM Probes .....	1507
Operational Commands .....	1511
monitor list .....	1512
monitor start .....	1513
monitor stop .....	1515
monitor traffic .....	1516
mtrace monitor .....	1526
ping mpls l2vpn .....	1528
ping mpls l2circuit .....	1531
ping mpls l3vpn .....	1534
ping mpls ldp .....	1536
ping mpls lsp-end-point .....	1539
ping mpls rsvp .....	1541
request pppoe connect .....	1546
request pppoe disconnect .....	1547
show configuration .....	1548
show chassis alarms .....	1551
show interfaces (SRX Series) .....	1553
show poe interface (View) .....	1582
show poe telemetries interface (View) .....	1584
show pppoe interfaces .....	1586
show pppoe statistics .....	1590
show security alarms .....	1592
show security datapath-debug capture .....	1596
show security datapath-debug counter .....	1597
show security monitoring fpc fpc-number .....	1598
show security monitoring performance session .....	1601
show security monitoring performance spu .....	1602
show services rpm probe-results (View) .....	1603
show system alarms .....	1607
traceroute .....	1608

	Troubleshooting .....	1611
	Troubleshooting Security Devices .....	1611
	Recovering the Root Password for J Series Devices .....	1612
	Recovering the Root Password for SRX Series Devices .....	1614
	Troubleshooting Access Manager Client-Side Problems .....	1615
	Troubleshooting DNS Name Resolution in Logical System Security Policies .....	1616
	Troubleshooting the Link Services Interface .....	1616
	Troubleshooting Security Policies .....	1625
	Troubleshooting the TGM550 Module and VoIP Interface .....	1627
	Troubleshooting ISSU-Related Problems Using Log Error Messages ..	1628
<b>Chapter 19</b>	<b>System Log Monitoring and Troubleshooting Guide for Security Devices .....</b>	<b>1633</b>
	Overview .....	1633
	System Log Messages .....	1633
	Junos OS System Log Configuration Overview .....	1633
	Junos OS Platform-Specific Default System Log Messages .....	1634
	Displaying and Interpreting System Log Message Descriptions .....	1635
	Interpreting Messages Generated in Structured-Data Format .....	1636
	Interpreting Messages Generated in Standard Format by Services on a PIC .....	1641
	Junos OS System Logging Facilities and Message Severity Levels ..	1642
	Security Devices .....	1643
	Understanding System Logging for Security Devices .....	1643
	Understanding Binary Format for Security Logs .....	1645
	Single-Chassis Systems .....	1646
	Displaying a Log File from a Single-Chassis System .....	1646
	The message-source Field on a Single-Chassis System .....	1646
	Configuration .....	1647
	System Log Messages .....	1647
	Examples: Configuring System Logging .....	1647
	Examples: Assigning an Alternative Facility .....	1649
	Examples: Displaying a Log File .....	1649
	Examples: Displaying System Log Message Descriptions .....	1650
	Security Devices .....	1651
	Configuring Binary Security Log Files .....	1651
	Sending System Log Messages to a File .....	1652
	Setting the System to Send All Log Messages Through eventd .....	1653
	Setting the System to Stream Security Logs Through Revenue Ports .....	1654
	Single-Chassis Systems .....	1654
	Junos OS Minimum System Logging Configuration .....	1655
	Junos OS Default System Log Settings .....	1656
	Junos OS Platform-Specific Default System Log Messages .....	1657
	Specifying the Facility and Severity of Messages to Include in the Log .....	1658
	Directing System Log Messages to a Log File .....	1658
	Logging Messages in Structured-Data Format .....	1659

Directing System Log Messages to a User Terminal . . . . .	1660
Directing System Log Messages to the Console . . . . .	1660
System Log Default Facilities for Messages Directed to a Remote Destination . . . . .	1660
Adding a Text String to System Log Messages . . . . .	1661
Adding a String . . . . .	1662
Including Priority Information in System Log Messages . . . . .	1662
Including the Year or Millisecond in Timestamps . . . . .	1663
Using Regular Expressions to Refine the Set of Logged Messages . . .	1664
Disabling the System Logging of a Facility . . . . .	1666
Configuration Statements . . . . .	1666
allow-duplicates . . . . .	1668
archive (All System Log Files) . . . . .	1669
cache (Security Log) . . . . .	1670
console (System Logging) . . . . .	1671
destination-override . . . . .	1672
event-rate . . . . .	1672
explicit-priority . . . . .	1673
exclude (Security Log) . . . . .	1674
facility-override . . . . .	1675
file (Security Log) . . . . .	1676
file (System Logging) . . . . .	1677
files . . . . .	1678
host (Security Log) . . . . .	1679
limit (Security Log) . . . . .	1679
log (Services) . . . . .	1680
log-prefix . . . . .	1681
log-rotate-frequency . . . . .	1681
match . . . . .	1682
mode (Security Log) . . . . .	1682
no-remote-trace . . . . .	1682
pic-services-logging . . . . .	1683
port . . . . .	1684
security-log . . . . .	1685
security-log-percent-full . . . . .	1685
severity (Security Log) . . . . .	1686
size . . . . .	1687
system . . . . .	1687
structured-data . . . . .	1688
syslog . . . . .	1689
time-format . . . . .	1691
traceoptions (Security Log) . . . . .	1692
tracing . . . . .	1694
user (System Logging) . . . . .	1695
world-readable . . . . .	1696

	Administration . . . . .	1696
	System Log Messages . . . . .	1696
	Monitoring System Log Messages with the J-Web Event Viewer . . . . .	1696
	Operational Commands . . . . .	1697
	clear log . . . . .	1699
	clear security log . . . . .	1700
	clear security log file . . . . .	1702
	monitor list . . . . .	1703
	monitor start . . . . .	1704
	monitor stop . . . . .	1706
	show log . . . . .	1707
	show security log . . . . .	1709
	show security log file . . . . .	1712
<b>Chapter 20</b>	<b>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1715</b>
	Overview . . . . .	1715
	SNMP . . . . .	1715
	Understanding the SNMP Implementation in Junos OS . . . . .	1716
	Standard SNMP MIBs Supported by Junos OS . . . . .	1719
	Juniper Networks Enterprise-Specific MIBs . . . . .	1733
	List of SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways Supported Enterprise-Specific MIBs . . . . .	1740
	List of SRX1400, SRX3400, and SRX3600 Services Gateways Supported Enterprise-Specific MIBs . . . . .	1745
	List of SRX5400, SRX5600 and SRX5800 Services Gateways Supported Enterprise-Specific MIBs . . . . .	1750
	Enterprise-Specific MIBs and Supported Devices . . . . .	1756
	MIB Support Details . . . . .	1766
	SNMP MIB Objects Supported by Junos OS for the Set Operation . . . . .	1775
	SNMPv3 . . . . .	1782
	SNMPv3 Overview . . . . .	1782
	Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage . . . . .	1783
	SNMP Traps . . . . .	1785
	Juniper Networks Enterprise-Specific SNMP Traps . . . . .	1785
	Standard SNMP Traps Supported on Devices Running Junos OS . . . . .	1785
	Standard SNMP Version 1 Traps . . . . .	1786
	Standard SNMP Version 2 Traps . . . . .	1789
	Unsupported Standard SNMP Traps . . . . .	1793
	Routing Instances . . . . .	1796
	Identifying a Routing Instance . . . . .	1797
	Understanding SNMP Support for Routing Instances . . . . .	1797
	Trap Support for Routing Instances . . . . .	1799
	Device Management . . . . .	1799
	Understanding Device Management Functions in Junos OS . . . . .	1799
	Understanding the Integrated Local Management Interface . . . . .	1801
	Remote Operations . . . . .	1801
	SNMP Remote Operations Overview . . . . .	1801

Remote Monitoring, Health Monitoring, and Service Quality . . . . .	1804
Understanding RMON Alarms . . . . .	1804
Understanding RMON Events . . . . .	1806
Understanding Measurement Points, Key Performance Indicators, and Baseline Values . . . . .	1807
Understanding RMON for Monitoring Service Quality . . . . .	1808
Configuration . . . . .	1812
SNMP . . . . .	1812
Configuring SNMP on a Device Running Junos OS . . . . .	1813
Configuring the System Contact on a Device Running Junos OS . . . . .	1815
Configuring the System Description on a Device Running Junos OS . . . . .	1815
Configuring the System Location for a Device Running Junos OS . . . . .	1816
Configuring the System Name . . . . .	1816
Configuring the Commit Delay Timer . . . . .	1817
Loading MIB Files to a Network Management System . . . . .	1817
Filtering Duplicate SNMP Requests . . . . .	1819
Configuring the Interfaces on Which SNMP Requests Can Be Accepted . . . . .	1820
Example: Configuring Secured Access List Checking . . . . .	1820
Filtering Interface Information Out of SNMP Get and GetNext Output . . . . .	1820
Configuring MIB Views . . . . .	1821
Example: Ping Proxy MIB . . . . .	1822
Configuring the Local Engine ID . . . . .	1823
Configuring SNMP Informs . . . . .	1823
SNMPv3 . . . . .	1824
Creating SNMPv3 Users . . . . .	1824
Example: SNMPv3 Configuration . . . . .	1825
Minimum SNMPv3 Configuration on a Device Running Junos OS . . . . .	1828
Configuring the SNMPv3 Authentication Type . . . . .	1830
Configuring the Encryption Type . . . . .	1831
Assigning Security Model and Security Name to a Group . . . . .	1833
Example: Security Group Configuration . . . . .	1834
Example: Configuring the Tag List . . . . .	1835
Example: Creating SNMPv3 Users Configuration . . . . .	1835
SNMP Traps . . . . .	1836
Configuring SNMP Trap Options . . . . .	1837
Configuring the Trap Notification Filter . . . . .	1840
Configuring SNMP Trap Groups . . . . .	1841
Configuring SNMP Trap Options and Groups on a Device Running Junos OS . . . . .	1843
Configuring SNMPv3 Traps on a Device Running Junos OS . . . . .	1844
Configuring the SNMPv3 Trap Notification . . . . .	1845
Example: Configuring SNMP Trap Groups . . . . .	1846
Configuring the Trap Target Address . . . . .	1846
Defining and Configuring the Trap Target Parameters . . . . .	1849
Example: Configuring SNMPv3 Trap Notification . . . . .	1852

Access Privileges . . . . .	1852
Defining Access Privileges for an SNMP Group . . . . .	1853
Configuring the Access Privileges Granted to a Group . . . . .	1854
Example: Access Privilege Configuration . . . . .	1857
Routing Instances . . . . .	1858
Enabling SNMP Access over Routing Instances . . . . .	1858
Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community . . . . .	1858
Example: Configuring Interface Settings for a Routing Instance . . . . .	1859
Configuring Access Lists for SNMP Access over Routing Instances . . . . .	1861
Community Strings . . . . .	1861
Configuring the SNMP Community String . . . . .	1862
Examples: Configuring the SNMP Community String . . . . .	1862
Adding a Group of Clients to an SNMP Community . . . . .	1863
Configuring the SNMPv3 Community . . . . .	1864
Example: SNMPv3 Community Configuration . . . . .	1866
Inform Notifications . . . . .	1867
Configuring the Inform Notification Type and Target Address . . . . .	1867
Example: Configuring the Inform Notification Type and Target Address . . . . .	1868
Remote Operations . . . . .	1869
Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS . . . . .	1869
Remote Monitoring, Health Monitoring, and Service Quality . . . . .	1869
Understanding RMON Alarms and Events Configuration . . . . .	1869
Configuring an Alarm Entry and Its Attributes . . . . .	1870
Configuring an Event Entry and Its Attributes . . . . .	1874
Example: Configuring an RMON Alarm and Event Entry . . . . .	1875
Configuring Health Monitoring on Devices Running Junos OS . . . . .	1875
Example: Configuring Health Monitoring . . . . .	1878
Configuration Statements . . . . .	1879
Configuration Statements at the [edit snmp] Hierarchy Level . . . . .	1882
Complete SNMPv3 Configuration Statements . . . . .	1885
access-list . . . . .	1887
address . . . . .	1888
address-mask . . . . .	1888
agent-address . . . . .	1889
alarm . . . . .	1890
authentication-md5 . . . . .	1891
authentication-none . . . . .	1892
authentication-password . . . . .	1893
authentication-sha . . . . .	1894
authorization . . . . .	1895
categories . . . . .	1895
client-list . . . . .	1896
client-list-name . . . . .	1896
clients . . . . .	1897
commit-delay . . . . .	1897
community . . . . .	1898

community	1899
community-name	1900
contact	1901
description	1901
description	1902
destination-port	1902
engine-id	1903
enterprise-oid	1904
event	1904
falling-event-index	1905
falling-threshold	1906
falling-threshold	1907
falling-threshold-interval	1908
filter-duplicates	1908
filter-interfaces	1909
group (Configuring Group Name)	1910
group (Defining Access Privileges for an SNMPv3 Group)	1911
health-monitor	1911
interface	1912
interval	1912
interval	1913
local-engine	1914
location	1915
logical-system	1916
logical-system-trap-filter	1917
message-processing-model	1917
name	1918
nonvolatile	1918
notify	1919
notify-filter (Applying to the Management Target)	1919
notify-filter (Configuring the Profile Name)	1920
notify-view	1920
oid	1921
oid	1921
parameters	1922
port	1922
privacy-3des	1923
privacy-aes128	1924
privacy-des	1925
privacy-none	1925
privacy-password	1926
read-view	1927
remote-engine	1928
request-type	1929
retry-count	1929
rising-event-index	1930
rising-threshold	1930
rising-threshold	1931
rmon	1931

routing-engine (SNMP Resource Level) . . . . .	1932
routing-engine (SNMP Global Level) . . . . .	1933
routing-instance . . . . .	1934
routing-instance . . . . .	1935
routing-instance-access . . . . .	1935
sample-type . . . . .	1936
security-level (Defining Access Privileges) . . . . .	1937
security-level (Generating SNMP Notifications) . . . . .	1938
security-model (Access Privileges) . . . . .	1939
security-model (Group) . . . . .	1940
security-model (SNMP Notifications) . . . . .	1940
security-name (Community String) . . . . .	1941
security-name (Security Group) . . . . .	1941
security-name (SNMP Notifications) . . . . .	1942
security-to-group . . . . .	1943
snmp . . . . .	1943
source-address . . . . .	1944
snmp-community . . . . .	1944
startup-alarm . . . . .	1945
syslog-subtag . . . . .	1945
tag . . . . .	1946
tag-list . . . . .	1946
target-address . . . . .	1947
target-parameters . . . . .	1948
targets . . . . .	1949
timeout . . . . .	1949
traceoptions . . . . .	1950
trap-group . . . . .	1952
trap-options . . . . .	1953
type . . . . .	1953
type . . . . .	1954
user . . . . .	1954
usm . . . . .	1955
v3 . . . . .	1957
vacm . . . . .	1959
variable . . . . .	1960
version . . . . .	1960
view (Associating a MIB View with a Community) . . . . .	1961
view (Configuring a MIB View) . . . . .	1962
write-view . . . . .	1963
Administration . . . . .	1963
SNMP Traps . . . . .	1963
Managing Traps and Informs . . . . .	1963
Remote Operations . . . . .	1966
Using the Ping MIB for Remote Monitoring Devices Running Junos OS . . . . .	1966
Configuring the Remote Engine and Remote User . . . . .	1966
Example: Configuring the Remote Engine ID and Remote Users . . . . .	1967



	Tracing Activity . . . . .	1968
	Tracing SNMP Activity on a Device Running Junos OS . . . . .	1968
	Example: Tracing SNMP Activity . . . . .	1971
	Ping Tests . . . . .	1972
	Starting a Ping Test . . . . .	1972
	Monitoring a Running Ping Test . . . . .	1973
	Gathering Ping Test Results . . . . .	1976
	Stopping a Ping Test . . . . .	1977
	Interpreting Ping Variables . . . . .	1977
	Operational Commands . . . . .	1978
	show snmp health-monitor . . . . .	1979
	show snmp health-monitor routing-engine history . . . . .	1985
	show snmp health-monitor routing-engine status . . . . .	1989
	show snmp mib (View) . . . . .	1991
<b>Chapter 21</b>	<b>IDP Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1995</b>
	Overview . . . . .	1995
	IDP Logging . . . . .	1995
	Understanding IDP Logging . . . . .	1995
	Understanding IDP Log Suppression Attributes . . . . .	1996
	Understanding IDP Log Information Usage on the IC Series UAC Appliance . . . . .	1997
	Packet Capture . . . . .	1997
	Understanding Security Packet Capture . . . . .	1998
	Tuning . . . . .	1998
	Performance and Capacity Tuning for IDP Overview . . . . .	1998
	Configuration . . . . .	1999
	IDP Logging . . . . .	1999
	Example: Configuring IDP Log Suppression Attributes . . . . .	1999
	Configuration Statements . . . . .	2000
	Security Configuration Statement Hierarchy . . . . .	2005
	[edit security idp] Hierarchy Level . . . . .	2007
	ack-number . . . . .	2017
	action (Security Application-Level DDoS) . . . . .	2018
	action (Security Rulebase IPS) . . . . .	2019
	active-policy . . . . .	2020
	action-profile . . . . .	2021
	alert . . . . .	2022
	allow-icmp-without-flow . . . . .	2022
	anomaly . . . . .	2023
	application (Security Custom Attack) . . . . .	2023
	application (Security Application-Level DDoS) . . . . .	2024
	application (Security IDP) . . . . .	2024
	application-ddos . . . . .	2025
	application-identification . . . . .	2026
	attack-type (Security Anomaly) . . . . .	2027
	attack-type (Security Chain) . . . . .	2028
	attack-type (Security IDP) . . . . .	2030
	attack-type (Security Signature) . . . . .	2034

attacks (Security Exempt Rulebase) .....	2038
attacks (Security IPS Rulebase) .....	2039
automatic (Security) .....	2040
cache-size (Security) .....	2040
category (Security Dynamic Attack Group) .....	2041
chain .....	2042
code .....	2043
content-decompression-max-memory-kb .....	2044
content-decompression-max-ratio .....	2045
context (Security Custom Attack) .....	2045
count (Security Custom Attack) .....	2046
custom-attack .....	2047
custom-attack-group .....	2052
custom-attack-groups (Security IDP) .....	2052
custom-attacks .....	2053
data-length .....	2053
datapath-debug .....	2054
description (Security IDP Policy) .....	2055
destination (Security IP Headers Attack) .....	2056
destination-address (Security IDP Policy) .....	2057
destination-except .....	2058
destination-port (Security Signature Attack) .....	2058
detect-shellcode .....	2059
detector .....	2059
direction (Security Custom Attack) .....	2060
direction (Security Dynamic Attack Group) .....	2061
download-timeout .....	2062
dynamic-attack-group .....	2063
dynamic-attack-groups (Security IDP) .....	2064
enable-all-qmodules .....	2064
enable-packet-pool .....	2065
expression .....	2065
false-positives .....	2066
filters .....	2067
flow (Security IDP) .....	2068
from-zone (Security IDP Policy) .....	2068
global (Security IDP) .....	2069
group-members .....	2070
header-length .....	2071
host (Security IDP Sensor Configuration) .....	2071
icmp (Security IDP Custom Attack) .....	2072
icmp (Security IDP Signature Attack) .....	2073
icmpv6 (Security IDP) .....	2074
identification (Security ICMP Headers) .....	2074
identification (Security IP Headers) .....	2075
idp (Application Services) .....	2075
idp (Security Alarms) .....	2076
idp-policy (Security) .....	2077
ignore-memory-overflow .....	2079

ignore-reassembly-overflow	2080
ignore-regular-expression	2080
include-destination-address	2081
install	2081
interval (Security IDP)	2082
ip (Security IDP Custom Attack)	2082
ip-action (Security Application-Level DDoS)	2083
ip-action (Security IDP Rulebase IPS)	2084
ip-block	2085
ip-close	2085
ip-connection-rate-limit	2086
ip-flags	2087
ip-notify	2087
ips	2088
ipv4 (Security IDP Signature Attack)	2089
ipv6 (Security IDP)	2090
key-protection (Security IDP Sensor Configuration)	2090
log (Security IDP)	2091
log (Security IDP Policy)	2091
log-attacks	2092
log-create	2092
log-errors	2093
log-supercede-min	2093
match (Security IDP Policy)	2094
match (Security Rulebase DDoS)	2095
max-flow-mem	2095
max-logs-operate	2096
max-packet-mem-ratio	2096
max-packet-memory-ratio	2097
max-reass-packet-memory-ratio	2097
max-sessions (Security Packet Log)	2098
max-tcp-session-packet-memory	2098
max-time-report	2099
max-timers-poll-ticks	2099
max-udp-session-packet-memory	2100
member (Security IDP)	2100
mss (Security IDP)	2101
negate	2101
nested-application (Security IDP)	2102
notification	2102
option (Security IDP)	2103
order (Security IDP)	2103
packet-log (Security IDP Policy)	2104
packet-log (Security IDP Sensor Configuration)	2105
pattern (Security IDP)	2105
performance	2106
policy-lookup-cache	2106
post-attack	2107
post-attack-timeout	2107

pre-attack	2108
pre-filter-shellcode	2108
predefined-attack-groups	2109
predefined-attacks	2109
process-ignore-s2c	2110
process-override	2110
process-port	2111
products	2111
protocol-binding	2112
protocol-name	2113
protocol (Security IDP IP Headers)	2114
protocol (Security IDP Signature Attack)	2115
re-assembler	2118
recommended-action	2119
refresh-timeout	2119
regexp	2120
reject-timeout	2120
reset (Security IDP)	2121
reset-on-policy	2121
rpc	2122
rule (Security Exempt Rulebase)	2123
rule (Security DDoS Rulebase)	2124
rule (Security IPS Rulebase)	2125
rulebase-ddos	2127
rulebase-exempt	2128
rulebase-ips	2129
scope (Security IDP Chain Attack)	2130
scope (Security IDP Custom Attack)	2131
security-package	2132
sensor-configuration	2133
sequence-number (Security IDP ICMP Headers)	2135
sequence-number (Security IDP TCP Headers)	2136
service (Security IDP Anomaly Attack)	2136
service (Security IDP Dynamic Attack Group)	2137
sessions	2137
severity (Security IDP Custom Attack)	2138
severity (Security IDP Dynamic Attack Group)	2139
severity (Security IDP IPS Rulebase)	2140
shellcode	2141
signature (Security IDP)	2142
source (Security IDP IP Headers)	2146
source-address (Security IDP Policy)	2147
source-address (Security IDP Sensor Configuration)	2147
source-except	2148
source-port (Security IDP)	2148
ssl-inspection	2149
start-log	2149
start-time (Security IDP)	2150
statistics (Security IDP)	2150

suppression	2151
target (Security IDP)	2152
tcp (Security IDP Protocol Binding)	2153
tcp (Security IDP Signature Attack)	2154
tcp-flags	2156
terminal	2157
test (Security IDP)	2157
then (Security IDP Policy)	2158
then (Security Rulebase DDos)	2159
time-binding	2160
timeout (Security IDP Policy)	2160
to-zone (Security IDP Policy)	2161
tos	2162
total-length	2163
total-memory	2163
traceoptions (Security Datapath Debug)	2164
traceoptions (Security IDP)	2166
ttl (Security IDP)	2168
tunable-name	2169
tunable-value	2170
type (Security IDP Dynamic Attack Group)	2170
type (Security IDP ICMP Headers)	2171
udp (Security IDP Protocol Binding)	2172
udp (Security IDP Signature Attack)	2173
urgent-pointer	2174
url (Security IDP)	2174
window-scale	2175
window-size	2176
Administration	2176
Alarms and Auditing	2176
IDP Alarms and Auditing	2176
Packet Capture	2177
Example: Configuring Security Packet Capture	2177
Example: Configuring Packet Capture for Datapath Debugging	2179
Verifying Security Packet Capture	2182
Tuning	2182
Configuring Session Capacity for IDP (CLI Procedure)	2182
Clear Commands	2183
clear security datapath-debug counters	2185
clear security idp	2186
clear security idp application-ddos cache	2187
clear security idp attack table	2188
clear security idp counters application-identification	2189
clear security idp counters dfa	2190
clear security idp counters flow	2191
clear security idp counters http-decoder	2192
clear security idp counters ips	2193
clear security idp counters log	2194
clear security idp counters packet	2195

clear security idp counters policy-manager . . . . .	2196
clear security idp counters tcp-reassembler . . . . .	2197
clear security idp ssl-inspection session-id-cache . . . . .	2198
Request Commands . . . . .	2198
request security datapath-debug capture start . . . . .	2199
request security idp security-package download . . . . .	2200
request security idp security-package install . . . . .	2202
request security idp ssl-inspection key add . . . . .	2204
request security idp ssl-inspection key delete . . . . .	2206
request security idp storage-cleanup . . . . .	2208
Show Commands . . . . .	2208
show security flow session idp family . . . . .	2210
show security flow session idp summary . . . . .	2212
show security idp active-policy . . . . .	2214
show security idp application-ddos application . . . . .	2215
show security idp attack description . . . . .	2217
show security idp attack detail . . . . .	2218
show security idp attack table . . . . .	2220
show security idp counters application-ddos . . . . .	2221
show security idp counters application-identification . . . . .	2224
show security idp counters dfa . . . . .	2226
show security idp counters flow . . . . .	2227
show security idp counters http-decoder . . . . .	2234
show security idp counters ips . . . . .	2235
show security idp counters log . . . . .	2238
show security idp counters packet . . . . .	2241
show security idp counters packet-log . . . . .	2244
show security idp counters policy-manager . . . . .	2246
show security idp counters tcp-reassembler . . . . .	2247
show security idp logical-system policy-association . . . . .	2250
show security idp memory . . . . .	2251
show security idp policies . . . . .	2252
show security idp policy-commit-status . . . . .	2253
show security idp policy-commit-status clear . . . . .	2254
show security idp policy-templates . . . . .	2255
show security idp predefined-attacks . . . . .	2256
show security idp security-package-version . . . . .	2258
show security idp ssl-inspection key . . . . .	2259
show security idp ssl-inspection session-id-cache . . . . .	2261
show security idp status . . . . .	2262
show security idp status detail . . . . .	2264

## Part 7

### Chapter 22

## Standards Reference

Overview . . . . .	2269
Accessing Standards Documents . . . . .	2269
Accessing Standards Documents on the Internet . . . . .	2269

<b>Chapter 23</b>	<b>Supported Standards</b>	<b>2271</b>
	Chassis and System Standards	2271
	Supported BOOTP and DHCP Standards	2271
	Supported Mobile IP Standards	2272
	Supported Network Management Standards	2273
	Supported RADIUS and TACACS+ Standards for User Authentication	2282
	Supported System Access Standards	2283
	Supported Time Synchronization Standard	2283
	Interface Standards	2284
	Supported ATM Interface Standards	2284
	Supported Ethernet Interface Standards	2284
	Supported Frame Relay Interface Standards	2285
	Supported GRE and IP-IP Interface Standards	2286
	Supported PPP Interface Standards	2286
	Supported SDH and SONET Interface Standards	2287
	Supported Serial Interface Standards	2288
	Supported T3 Interface Standard	2288
	Layer 2 Standards	2289
	Supported Layer 2 Networking Standards	2289
	Supported L2TP Standards	2289
	Supported Layer 2 Circuit Standards	2290
	Supported Layer 2 VPN Standard	2290
	MPLS Applications Standards	2291
	Supported GMPLS Standards	2291
	Supported LDP Standards	2292
	Supported MPLS Standards	2293
	Supported RSVP Standards	2295
	Packet Processing Standards	2296
	Supported CoS Standards	2296
	Supported Packet Filtering Standards	2297
	Supported Policing Standard	2297
	Routing Protocol Standards	2298
	Supported BGP Standards	2298
	Supported ES-IS Standards	2300
	Supported ICMP and Neighbor Discovery Standards	2300
	Supported IP Multicast Protocol Standards	2301
	Supported IPv4, TCP, and UDP Standards	2302
	Supported IPv6 Standards	2303
	Supported IS-IS Standards	2306
	Supported OSPF and OSPFv3 Standards	2307
	Supported RIP and RIPvng Standards	2309
	Services PIC and DPC Standards	2309
	Supported DTCP Standard	2309
	Supported Flow Monitoring and Discard Accounting Standards	2310
	Supported IPsec and IKE Standards	2310
	Supported L2TP Standards	2311
	Supported Link Services Standards	2311
	Supported NAT and SIP Standards	2312
	Supported RPM Standard	2312

Supported Voice Services Standards . . . . .	2313
VPLS and VPN Standards . . . . .	2313
Supported Carrier-of-Carriers and Interprovider VPN Standards . . . . .	2313
Supported Layer 2 VPN Standard . . . . .	2313
Supported Layer 3 VPN Standards . . . . .	2314
Supported Multicast VPN Standards . . . . .	2315
Supported VPLS Standards . . . . .	2315

## Part 8

## Index

Index . . . . .	2319
-----------------	------



# List of Figures

<b>Part 1</b>	<b>Junos OS Getting Started Guide for Branch SRX Series</b>	
<b>Chapter 1</b>	<b>Overview</b>	<b>3</b>
	Figure 1: SRX210 Deployment Topology	4
<b>Chapter 2</b>	<b>Configuration</b>	<b>15</b>
	Figure 2: Connecting a Branch SRX Series Services Gateway to the Internet	20
	Figure 3: Connecting a Branch SRX Series Services Gateway to the Internet	28
	Figure 4: Topology for Security Policy Configuration	39
	Figure 5: Destination NAT Single Address Translation	44
<b>Part 2</b>	<b>Installation and Upgrade Guide for Security Devices</b>	
<b>Chapter 4</b>	<b>Overview</b>	<b>129</b>
	Figure 6: J Series Services Routers (J4300 Shown)	134
<b>Chapter 5</b>	<b>Installation</b>	<b>163</b>
	Figure 7: Connecting to the Console Port on a Junos OS Device	171
<b>Part 3</b>	<b>CLI User Guide</b>	
<b>Chapter 8</b>	<b>Overview</b>	<b>309</b>
	Figure 8: Monitoring and Configuring Routers	310
	Figure 9: Committing a Configuration	312
	Figure 10: Configuration Statement Hierarchy Example	313
	Figure 11: Commands That Combine Other Commands	322
	Figure 12: Command Output Options	323
	Figure 13: Configuration Mode Hierarchy of Statements	339
<b>Chapter 9</b>	<b>Configuration</b>	<b>357</b>
	Figure 14: Confirm a Configuration	410
	Figure 15: Overriding the Current Configuration	424
	Figure 16: Using the replace Option	424
	Figure 17: Using the merge Option	424
	Figure 18: Using a Patch File	425
	Figure 19: Using the set Option	425
	Figure 20: Replacement by Object	458
<b>Chapter 10</b>	<b>Administration</b>	<b>493</b>
	Figure 21: Restarting a Process	506
<b>Part 4</b>	<b>J-Web User Guide</b>	
<b>Chapter 12</b>	<b>Overview</b>	<b>579</b>

	Figure 22: J-Web Layout . . . . .	580
	Figure 23: Top Pane Elements . . . . .	581
	Figure 24: Main Pane Elements . . . . .	582
	Figure 25: Side Pane Elements . . . . .	583
	Figure 26: CoS Help Page . . . . .	585
	Figure 27: J-Web Set Up Initial Configuration Page . . . . .	589
<b>Chapter 13</b>	<b>Configuration . . . . .</b>	<b>593</b>
	Figure 28: View Configuration Text Page . . . . .	598
	Figure 29: Edit Configuration Text Page . . . . .	599
	Figure 30: Starting the CLI Terminal . . . . .	601
	Figure 31: J-Web CLI Terminal . . . . .	603
	Figure 32: Edit Configuration Page . . . . .	605
	Figure 33: Accounting Options Configuration Editor Page . . . . .	609
<b>Chapter 14</b>	<b>Administration . . . . .</b>	<b>611</b>
	Figure 34: Edit Management Access Page . . . . .	613
	Figure 35: View Alarms Page . . . . .	617
	Figure 36: View Events page . . . . .	618
	Figure 37: J-Web View Events Page . . . . .	623
	Figure 38: Manage Snapshots Page . . . . .	627
	Figure 39: Chassis Viewer Page . . . . .	629
	Figure 40: Sample RPM Graphs . . . . .	633
	Figure 41: Port Monitoring Page . . . . .	639
	Figure 42: Details of Interface ge-0/0/0 Page . . . . .	640
	Figure 43: Monitoring Route Information Page with Complete Information . . . . .	641
	Figure 44: Monitoring Route Information Page with Selective Information . . . . .	641
	Figure 45: Configuration Database and History Page . . . . .	643
	Figure 46: Database Information Page . . . . .	645
	Figure 47: J-Web Configuration File Comparison Results . . . . .	647
	Figure 48: J-Web Upload Configuration File Page . . . . .	648
	Figure 49: Rescue Configuration Page . . . . .	648
<b>Chapter 15</b>	<b>Troubleshooting . . . . .</b>	<b>651</b>
	Figure 50: View Events Page Displaying Error . . . . .	652
	Figure 51: Verifying System Log Messages Configuration . . . . .	653
	Figure 52: Ping Host Troubleshoot Page . . . . .	658
	Figure 53: Successful Ping Host Results Page . . . . .	658
	Figure 54: Unsuccessful Ping Host Results Page . . . . .	659
<b>Part 6</b>	<b>Monitoring and Troubleshooting Library for Security Devices</b>	
<b>Chapter 18</b>	<b>Network Monitoring and Troubleshooting Guide for Security Devices . . .</b>	<b>1231</b>
	Figure 55: Sample RPM Graphs . . . . .	1508
	Figure 56: Connecting to the Console Port on the J Series Device . . . . .	1612
	Figure 57: PPP and MLPPP Headers . . . . .	1621
<b>Chapter 20</b>	<b>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1715</b>
	Figure 58: SNMP Data for Routing Instances . . . . .	1798
	Figure 59: Network Entry Points . . . . .	1807

Figure 60: Setting Thresholds . . . . .	1809
Figure 61: Inform Request and Response . . . . .	1824



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>lvii</b>
	Table 1: Notice Icons . . . . .	lix
	Table 2: Text and Syntax Conventions . . . . .	lix
<b>Part 1</b>	<b>Junos OS Getting Started Guide for Branch SRX Series</b>	
<b>Chapter 1</b>	<b>Overview</b> . . . . .	<b>3</b>
	Table 3: Default Interfaces Settings . . . . .	5
	Table 4: Default Security Policy Settings . . . . .	5
	Table 5: Default NAT Settings . . . . .	6
	Table 6: Factory-Default Settings for Security Policies for Branch SRX Series Devices . . . . .	9
	Table 7: Default UTM Profiles on Branch SRX Series . . . . .	11
<b>Chapter 2</b>	<b>Configuration</b> . . . . .	<b>15</b>
	Table 8: Settings Used to Configure the SRX210 . . . . .	15
	Table 9: Address Books Configuration . . . . .	40
	Table 10: Security Policy Configuration . . . . .	40
	Table 11: Destination NAT Mapping . . . . .	45
<b>Chapter 3</b>	<b>Administration</b> . . . . .	<b>89</b>
	Table 12: show security idp active-policy Output Fields . . . . .	99
	Table 13: show security idp status Output Fields . . . . .	100
	Table 14: show security flow session Output Fields . . . . .	103
	Table 15: show security nat destination summary Output Fields . . . . .	107
	Table 16: show security policies Output Fields . . . . .	110
	Table 17: show security zones Output Fields . . . . .	118
	Table 18: show system license Output Fields . . . . .	121
	Table 19: show system services dhcp client Output Fields . . . . .	124
<b>Part 2</b>	<b>Installation and Upgrade Guide for Security Devices</b>	
<b>Chapter 4</b>	<b>Overview</b> . . . . .	<b>129</b>
	Table 20: Routing Engines and Storage Media Names (J Series Routers) . . . . .	135
	Table 21: show system download Output Fields . . . . .	144
	Table 22: Storage Media on SRX Series Devices . . . . .	146
	Table 23: Autorecovery Alarms . . . . .	148
	Table 24: CLI Commands for Manual BIOS Upgrade . . . . .	150
	Table 25: Interfaces and Protocols for IP Address Acquisition During Autoinstallation . . . . .	152
	Table 26: Summary of License Management Fields . . . . .	157
	Table 27: Junos OS Feature Licenses . . . . .	160

<b>Chapter 5</b>	<b>Installation</b> .....	<b>163</b>
	Table 28: Secondary Storage Devices for SRX Series Devices .....	166
	Table 29: Secondary Storage Devices for Backup .....	167
	Table 30: Environment Variables Settings .....	182
	Table 31: Install Package Summary .....	186
	Table 32: Install Remote Summary .....	187
<b>Chapter 6</b>	<b>Configuration</b> .....	<b>205</b>
	Table 33: CLI set system dump-device Command Options .....	208
<b>Chapter 7</b>	<b>Administration</b> .....	<b>253</b>
	Table 34: show system autorecovery state Output Fields .....	292
	Table 35: show system auto-snapshot Output Fields .....	294
	Table 36: show system download Output Fields .....	296
	Table 37: show system license Output Fields .....	298
	Table 38: show system login lockout .....	301
	Table 39: show system storage Output Fields .....	303
<b>Part 3</b>	<b>CLI User Guide</b>	
<b>Chapter 8</b>	<b>Overview</b> .....	<b>309</b>
	Table 40: CLI Configuration Mode Navigation Commands .....	313
	Table 41: Commonly Used Operational Mode Commands .....	320
	Table 42: Common Regular Expression Operators in Operational Mode Commands .....	328
	Table 43: Summary of Configuration Mode Commands .....	336
	Table 44: Configuration Mode Top-Level Statements .....	338
	Table 45: Forms of the configure Command .....	343
	Table 46: CLI Configuration Input Types .....	346
	Table 47: CLI Keyboard Sequences .....	347
	Table 48: Wildcard Characters for Specifying Interface Names .....	349
<b>Chapter 10</b>	<b>Administration</b> .....	<b>493</b>
	Table 49: Directories on the Router .....	498
	Table 50: show system process extensive Command Output Fields .....	505
	Table 51: Commonly Used Operational Mode Commands .....	513
	Table 52: Common Regular Expressions to Use with the replace Command ..	516
	Table 53: Replacement Examples .....	516
	Table 54: show cli Output Fields .....	528
	Table 55: show system commit Output Fields .....	567
<b>Part 4</b>	<b>J-Web User Guide</b>	
<b>Chapter 12</b>	<b>Overview</b> .....	<b>579</b>
	Table 56: Key J-Web Edit Configuration Buttons .....	584
	Table 57: Initial Configuration Set Up Summary .....	589
<b>Chapter 13</b>	<b>Configuration</b> .....	<b>593</b>
	Table 58: Junos OS Configuration Terms .....	594
	Table 59: J-Web Configuration Editor Tasks Summary .....	595
	Table 60: J-Web Configuration Tasks Summary .....	604

	Table 61: J-Web Edit Configuration Links . . . . .	606
	Table 62: J-Web Edit Configuration Icons . . . . .	606
	Table 63: J-Web Edit Configuration Buttons . . . . .	607
<b>Chapter 14</b>	<b>Administration . . . . .</b>	<b>611</b>
	Table 64: Secure Access Configuration Summary . . . . .	613
	Table 65: Severity Levels . . . . .	619
	Table 66: Summary of Event Filters . . . . .	620
	Table 67: Common Regular Expression Operators and the Terms They Match . . . . .	621
	Table 68: Manage Software Tasks Summary . . . . .	624
	Table 69: Class of Service Information and the Corresponding CLI show Commands . . . . .	630
	Table 70: Interfaces Information and the Corresponding CLI show Commands . . . . .	631
	Table 71: MPLS Information and the Corresponding CLI show Commands . . . .	631
	Table 72: PPPoE Information and the Corresponding CLI show Commands . . .	632
	Table 73: RPM Information and the Corresponding CLI show Command . . . . .	632
	Table 74: Routing Information and the Corresponding CLI show Commands . .	633
	Table 75: Firewall Information and the Corresponding CLI show Commands . .	634
	Table 76: IPsec Information and the Corresponding CLI show Commands . . .	635
	Table 77: NAT Information and the Corresponding CLI show Command . . . . .	635
	Table 78: Service Sets Information and the Corresponding CLI show Commands . . . . .	636
	Table 79: DHCP Information and the Corresponding CLI show Commands . . .	636
	Table 80: System Information and the Corresponding CLI show Commands . .	637
	Table 81: Chassis Information and the Corresponding CLI show Commands . .	637
	Table 82: Process Details Information and the Corresponding CLI show Commands . . . . .	638
	Table 83: FEB Redundancy Information and the Corresponding CLI show Command . . . . .	638
	Table 84: J-Web Configuration History Summary . . . . .	643
	Table 85: J-Web Configuration Database Information Summary . . . . .	645
	Table 86: Manage Files Tasks Summary . . . . .	649
<b>Chapter 15</b>	<b>Troubleshooting . . . . .</b>	<b>651</b>
	Table 87: Ping MPLS Tasks Summary and the Corresponding CLI show Commands . . . . .	655
	Table 88: J-Web Ping Host Results and Output Summary . . . . .	658
<b>Part 5</b>	<b>Administration Library for Security Devices</b>	
<b>Chapter 16</b>	<b>Administration Guide for Security Devices . . . . .</b>	<b>663</b>
	Table 89: Concurrent Web Sessions on SRX Series Devices . . . . .	666
	Table 90: Predefined Login Classes . . . . .	673
	Table 91: Permission Bits for Login Classes . . . . .	674
	Table 92: Default Modem Initialization Commands . . . . .	678
	Table 93: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity . . . . .	680
	Table 94: Incoming Map Options . . . . .	681

	Table 95: Sample DHCP Configuration Settings . . . . .	685
	Table 96: Summary of License Management Fields . . . . .	697
	Table 97: Junos OS Feature Licenses . . . . .	698
	Table 98: DHCPv6 Attributes . . . . .	749
	Table 99: CLI telnet Command Options . . . . .	928
	Table 100: CLI ssh Command Options . . . . .	929
	Table 101: request system set-encryption-key Commands . . . . .	933
	Table 102: Sample show Commands Called by the request information support command on an MX Series Router . . . . .	996
	Table 103: show chassis routing-engine Output Fields . . . . .	1012
	Table 104: show dhcp client binding Output Fields . . . . .	1014
	Table 105: show dhcpv6 client binding Output Fields . . . . .	1017
	Table 106: show dhcp client statistics . . . . .	1019
	Table 107: show dhcpv6 client statistics Output Fields . . . . .	1021
	Table 108: show dhcp relay binding Output Fields . . . . .	1023
	Table 109: show dhcp relay statistics . . . . .	1025
	Table 110: show dhcp server binding Output Fields . . . . .	1027
	Table 111: show dhcp server statistics . . . . .	1029
	Table 112: show dhcv6p server binding Output Fields . . . . .	1031
	Table 113: show dhcpv6 server statistics Output Fields . . . . .	1036
	Table 114: show firewall Output Fields . . . . .	1038
	Table 115: show system autorecovery state Output Fields . . . . .	1040
	Table 116: show system directory-usage Output Fields . . . . .	1042
	Table 117: show system download Output Fields . . . . .	1044
	Table 118: show system license Output Fields . . . . .	1046
	Table 119: show system login logout . . . . .	1049
	Table 120: show system services dhcp client Output Fields . . . . .	1050
	Table 121: show system services dhcp relay-statistics Output Fields . . . . .	1053
	Table 122: show system storage Output Fields . . . . .	1056
<b>Chapter 17</b>	<b>Access Privilege Administration Guide . . . . .</b>	<b>1059</b>
	Table 123: Login Class Permission Flags . . . . .	1060
	Table 124: Predefined System Login Classes . . . . .	1064
<b>Part 6</b>	<b>Monitoring and Troubleshooting Library for Security Devices</b>	
<b>Chapter 18</b>	<b>Network Monitoring and Troubleshooting Guide for Security Devices . . .</b>	<b>1231</b>
	Table 125: J-Web Interface Troubleshoot Options . . . . .	1233
	Table 126: CLI Diagnostic Command Summary . . . . .	1234
	Table 127: Types of Accounting Profiles . . . . .	1235
	Table 128: Interface Alarm Conditions . . . . .	1238
	Table 129: System Alarm Conditions and Corrective Actions . . . . .	1241
	Table 130: Options for Checking MPLS Connections . . . . .	1244
	Table 131: RPM Statistics . . . . .	1250
	Table 132: RPM Configuration Summary . . . . .	1306
	Table 133: CLI mtrace from-source Command Options . . . . .	1356
	Table 134: CLI mtrace from-source Command Output Summary . . . . .	1357
	Table 135: CLI monitor interface Output Control Keys . . . . .	1358
	Table 136: CLI monitor interface traffic Output Control Keys . . . . .	1359
	Table 137: CLI traceroute monitor Command Options . . . . .	1360



Table 138: CLI traceroute monitor Command Output Summary . . . . .	1361
Table 139: Address Pools Monitoring Page . . . . .	1362
Table 140: Summary of Key CoS Interfaces Output Fields . . . . .	1368
Table 141: Summary of Key CoS Classifier Output Fields . . . . .	1368
Table 142: Summary of Key CoS Value Alias Output Fields . . . . .	1370
Table 143: Summary of Key CoS RED Drop Profile Output Fields . . . . .	1370
Table 144: Summary of Key CoS Forwarding Class Output Fields . . . . .	1372
Table 145: Summary of Key CoS Rewrite Rules Output Fields . . . . .	1372
Table 146: Summary of Key CoS Scheduler Maps Output Fields . . . . .	1373
Table 147: Summary of Key CoS Classifier Output Fields . . . . .	1375
Table 148: Summary of Key DHCP Client Binding Output Fields . . . . .	1377
Table 149: Summary of Ethernet Switching Output Fields . . . . .	1377
Table 150: Events Monitoring Page . . . . .	1379
Table 151: GVRP Monitoring Page . . . . .	1381
Table 152: Summary of Key H.323 Counters Output Fields . . . . .	1381
Table 153: Summary of Key MGCP Calls Output Fields . . . . .	1384
Table 154: Summary of Key MGCP Counters Output Fields . . . . .	1385
Table 155: Summary of Key MGCP Endpoints Output Fields . . . . .	1386
Table 156: Summary of Key MPLS Interface Information Output Fields . . . . .	1387
Table 157: Summary of Key MPLS LSP Information Output Fields . . . . .	1388
Table 158: Summary of Key MPLS LSP Statistics Output Fields . . . . .	1389
Table 159: Summary of Key RSVP Session Information Output Fields . . . . .	1390
Table 160: Summary of Key RSVP Interfaces Information Output Fields . . . . .	1391
Table 161: Source NAT Monitoring Page . . . . .	1392
Table 162: Summary of Key Destination NAT Output Fields . . . . .	1398
Table 163: Summary of Key Static NAT Output Fields . . . . .	1400
Table 164: Summary of Key Incoming Table Output Fields . . . . .	1401
Table 165: Summary of Key Interface NAT Output Fields . . . . .	1402
Table 166: Summary of Key PPPoE Output Fields . . . . .	1404
Table 167: Statistics Tab Output in the Threats Report . . . . .	1407
Table 168: Activities Tab Output in the Threats Report . . . . .	1410
Table 169: Traffic Report Output . . . . .	1412
Table 170: Filtering Route Messages . . . . .	1414
Table 171: Summary of Key Routing Information Output Fields . . . . .	1415
Table 172: Summary of Key RIP Routing Output Fields . . . . .	1416
Table 173: Summary of Key OSPF Routing Output Fields . . . . .	1417
Table 174: Summary of Key BGP Routing Output Fields . . . . .	1419
Table 175: Summary of Key SCCP Calls Output Fields . . . . .	1421
Table 176: Summary of Key SCCP Counters Output Fields . . . . .	1421
Table 177: View Policy Log Fields . . . . .	1423
Table 178: Policy Events Detail Fields . . . . .	1424
Table 179: Security Policies Monitoring Output Fields . . . . .	1425
Table 180: Check Policies Output . . . . .	1428
Table 181: Summary of Key Screen Counters Output Fields . . . . .	1430
Table 182: Summary of IDP Status Output Fields . . . . .	1433
Table 183: Summary of Key Flow Gate Output Fields . . . . .	1434
Table 184: Summary of Key Firewall Authentication Table Output Fields . . . . .	1435
Table 185: Summary of Key Firewall Authentication History Output Fields . . . . .	1436
Table 186: Summary of Dot1X Output Fields . . . . .	1438

Table 187: Summary of Key SIP Calls Output Fields . . . . .	1439
Table 188: Summary of Key SIP Counters Output Fields . . . . .	1440
Table 189: Summary of Key SIP Rate Output Fields . . . . .	1442
Table 190: Summary of Key SIP Transactions Output Fields . . . . .	1442
Table 191: Spanning Tree Monitoring Page . . . . .	1443
Table 192: ALG H.323 Monitoring Page . . . . .	1452
Table 193: Voice ALG MGCP Monitoring Page . . . . .	1455
Table 194: Voice ALG SCCP Monitoring Page . . . . .	1457
Table 195: Voice ALG SIP Monitoring Page . . . . .	1460
Table 196: Voice ALG Summary Monitoring Page . . . . .	1465
Table 197: Summary of Key IKE SA Information Output Fields . . . . .	1466
Table 198: IPsec VPN—Phase I Monitoring Page . . . . .	1469
Table 199: IPsec VPN—Phase II Monitoring Page . . . . .	1470
Table 200: Summary of Key IPsec VPN Information Output Fields . . . . .	1472
Table 201: Alarms Monitoring Page . . . . .	1478
Table 202: CLI traceroute Command Options . . . . .	1480
Table 203: CLI mtrace monitor Command Output Summary . . . . .	1482
Table 204: Traceroute Field Summary . . . . .	1483
Table 205: J-Web Traceroute Results and Output Summary . . . . .	1484
Table 206: CLI ping Command Options . . . . .	1486
Table 207: J-Web Ping Host Field Summary . . . . .	1488
Table 208: Ping Host Results and Output . . . . .	1490
Table 209: J-Web Ping MPLS Field Summary . . . . .	1491
Table 210: J-Web Ping MPLS Results and Output Summary . . . . .	1494
Table 211: CLI ping mpls l2circuit Command Options . . . . .	1495
Table 212: CLI ping mpls l2vpn Command Options . . . . .	1496
Table 213: CLI ping mpls l3vpn Command Options . . . . .	1497
Table 214: CLI ping mpls ldp and ping mpls lsp-end-point Command Options . . . . .	1498
Table 215: CLI monitor traffic Command Options . . . . .	1499
Table 216: CLI monitor traffic Match Conditions . . . . .	1501
Table 217: CLI monitor traffic Logical Operators . . . . .	1502
Table 218: CLI monitor traffic Arithmetic, Binary, and Relational Operators . . . . .	1503
Table 219: Packet Capture Field Summary . . . . .	1504
Table 220: J-Web Packet Capture Results and Output Summary . . . . .	1507
Table 221: Summary of Key RPM Output Fields . . . . .	1508
Table 222: monitor list Output Fields . . . . .	1512
Table 223: monitor start Output Fields . . . . .	1513
Table 224: Match Conditions for the monitor traffic Command . . . . .	1518
Table 225: Logical Operators for the monitor traffic Command . . . . .	1519
Table 226: Arithmetic and Relational Operators for the monitor traffic Command . . . . .	1521
Table 227: mtrace monitor Output Fields . . . . .	1526
Table 228: show chassis alarms Output Fields . . . . .	1551
Table 229: show interfaces Output Fields . . . . .	1555
Table 230: show poe interface Output Fields . . . . .	1582
Table 231: show poe telemetries interface Output Fields . . . . .	1584
Table 232: show pppoe interfaces Output Fields . . . . .	1586
Table 233: show pppoe statistics Output Fields . . . . .	1590
Table 234: show security alarms . . . . .	1593

	Table 235: show security monitoring fpc fpc-number Output Fields . . . . .	1598
	Table 236: show services rpm probe-results Output Fields . . . . .	1603
	Table 237: traceroute Output Fields . . . . .	1610
	Table 238: CoS Components Applied on Multilink Bundles and Constituent Links . . . . .	1617
	Table 239: PPP and MLPPP Encapsulation Overhead . . . . .	1621
	Table 240: Number of Packets Transmitted on a Queue . . . . .	1624
<b>Chapter 19</b>	<b>System Log Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1633</b>
	Table 241: Fields in System Log Message Descriptions . . . . .	1635
	Table 242: Fields in Structured-Data Messages . . . . .	1637
	Table 243: Facility and Severity Codes in the priority-code Field . . . . .	1638
	Table 244: Platform Identifiers in the platform Field . . . . .	1640
	Table 245: Fields in Messages Generated by a PIC . . . . .	1641
	Table 246: Junos OS System Logging Facilities . . . . .	1642
	Table 247: System Log Message Severity Levels . . . . .	1643
	Table 248: Minimum Configuration Statements for System Logging . . . . .	1655
	Table 249: Default System Logging Settings . . . . .	1656
	Table 250: Default Facilities for Messages Directed to a Remote Destination . .	1660
	Table 251: Regular Expression Operators for the match Statement . . . . .	1665
	Table 252: monitor list Output Fields . . . . .	1703
	Table 253: monitor start Output Fields . . . . .	1704
	Table 254: show security log Output Fields . . . . .	1710
	Table 255: show security log file Output Fields . . . . .	1712
<b>Chapter 20</b>	<b>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1715</b>
	Table 256: Standard MIBs Supported on Devices Running Junos OS . . . . .	1720
	Table 257: Enterprise-Specific MIBs and Supported Devices . . . . .	1757
	Table 258: MIB Support for Routing Instances (Juniper Networks MIBs) . . . . .	1766
	Table 259: Class 1 MIB Objects (Standard and Juniper MIBs) . . . . .	1769
	Table 260: Class 2 MIB Objects (Standard and Juniper MIBs) . . . . .	1773
	Table 261: Class 3 MIB Objects (Standard and Juniper MIBs) . . . . .	1774
	Table 262: Class 4 MIB Objects (Standard and Juniper MIBs) . . . . .	1775
	Table 263: Standard Supported SNMP Version 1 Traps . . . . .	1786
	Table 264: Standard Supported SNMP Version 2 Traps . . . . .	1789
	Table 265: Unsupported Standard SNMP Traps . . . . .	1794
	Table 266: Device Management Features in Junos OS . . . . .	1800
	Table 267: RMON Event Table . . . . .	1810
	Table 268: RMON Alarm Table . . . . .	1811
	Table 269: jnxRmon Alarm Extensions . . . . .	1811
	Table 270: Monitored Object Instances . . . . .	1876
	Table 271: SNMP Tracing Flags . . . . .	1970
	Table 272: Results in pingProbeHistoryTable: After the First Ping Test . . . . .	1976
	Table 273: Results in pingProbeHistoryTable: After the First Probe of the Second Test . . . . .	1977
	Table 274: Results in pingProbeHistoryTable: After the Second Ping Test . . . . .	1977
	Table 275: show snmp health-monitor Output Fields . . . . .	1979
	Table 276: show snmp health-monitor routing engine history Output Fields . .	1985

**Chapter 21**

Table 277: show snmp health-monitor routing engine status Output Fields . . .	1989
Table 278: show snmp mib Output Fields . . . . .	1991
<b>IDP Monitoring and Troubleshooting Guide for Security Devices . . . . .</b>	<b>1995</b>
Table 279: show security flow session summary Output Fields . . . . .	2210
Table 280: show security flow session idp summary Output Fields . . . . .	2212
Table 281: show security idp active-policy Output Fields . . . . .	2214
Table 282: show security idp application-ddos Output Fields . . . . .	2215
Table 283: show security idp attack description Output Fields . . . . .	2217
Table 284: show security idp attack detail Output Fields . . . . .	2218
Table 285: show security idp attack table Output Fields . . . . .	2220
Table 286: show security idp counters application-ddos Output Fields . . . . .	2221
Table 287: show security idp counters application-identification Output Fields . . . . .	2224
Table 288: show security idp counters dfa Output Fields . . . . .	2226
Table 289: show security idp counters flow Output Fields . . . . .	2227
Table 290: show security idp counters http-decoder Output Fields . . . . .	2234
Table 291: show security idp counters ips Output Fields . . . . .	2235
Table 292: show security idp counters log Output Fields . . . . .	2238
Table 293: show security idp counters packet Output Fields . . . . .	2241
Table 294: show security idp counters policy-manager Output Fields . . . . .	2246
Table 295: show security idp counters tcp-reassembler Output Fields . . . . .	2247
Table 296: show security idp logical-system policy-association Output Fields . . . . .	2250
Table 297: show security idp memory Output Fields . . . . .	2251
Table 298: show security idp security-package-version Output Fields . . . . .	2258
Table 299: show security idp ssl-inspection key Output Fields . . . . .	2259
Table 300: show security idp ssl-inspection session-id-cache Output Fields . .	2261
Table 301: show security idp status Output Fields . . . . .	2262

# About the Documentation

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

## 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 lix](#) 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 lix](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>

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> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"><li>Introduces or emphasizes important new terms.</li><li>Identifies guide names.</li><li>Identifies RFC and Internet draft titles.</li></ul>	<ul style="list-style-type: none"><li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li><li><i>Junos OS CLI User Guide</i></li><li>RFC 1997, <i>BGP Communities Attribute</i></li></ul>
<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@# <b>set system domain-name</b> <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"><li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(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.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
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"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>



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 <b>Protocols&gt;Ospf</b> .

## 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](mailto: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](#)
- [Configuration on page 15](#)
- [Administration on page 89](#)



## CHAPTER 1

# Overview

- [SRX Series Basics on page 3](#)
- [SRX Series Security on page 7](#)

## SRX Series Basics

---

- [SRX Series Overview on page 3](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Understanding Methods to Manage Your Branch SRX Series on page 6](#)

## 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 3](#)
- [Understanding Methods to Manage Your Branch SRX Series on page 6](#)

## Understanding Factory Default Configuration Settings of an SRX210

This topic includes the following sections:

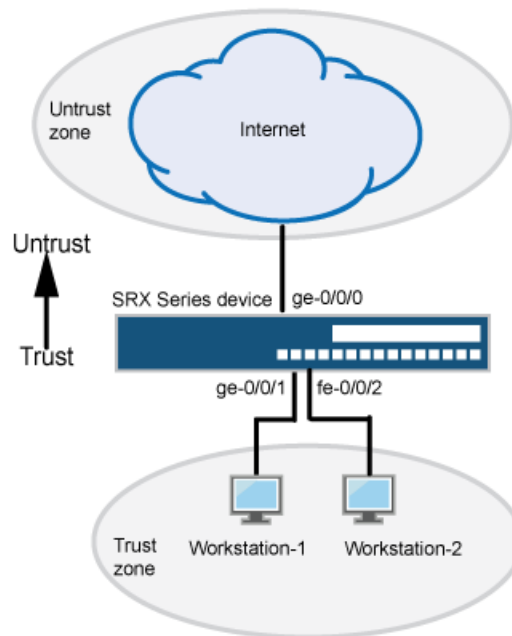
- [Default Configuration Topology on page 4](#)
- [Default Port Settings on page 5](#)
- [Default Settings for Interfaces, Zones, Policy, and NAT on page 5](#)

- [Default System Services on page 6](#)
- [Autoinstallation on page 6](#)

### Default Configuration Topology

Figure 1 on page 4 provides a topology of a simple network consisting of the SRX210.

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 5 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 5 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 6 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 Setting—A Sample” on page 34 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 “Autoinstallation Overview” on page 151.

#### Related Documentation

- [SRX Series Overview on page 3](#)
- [SRX210 Factory Default Setting—A Sample on page 34](#)
- [Understanding Methods to Manage Your Branch SRX Series on page 6](#)

## Understanding Methods to Manage Your 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” on page 16](#).

#### Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)

## SRX Series Security

- [Understanding Branch SRX Series Stateful Firewall Functionality on page 7](#)
- [Understanding Security Zones and Policies for SRX Series on page 8](#)
- [Understanding NAT for SRX Series on page 9](#)
- [Understanding Unified Threat Management for Branch SRX Series on page 10](#)
- [Understanding Intrusion Detection and Prevention for SRX Series on page 12](#)
- [Understanding IPsec VPN for SRX Series on page 12](#)
- [Understand Chassis Cluster for SRX Series on page 13](#)

### 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 8](#)
- [Example: Configuring Security Zones and Policies for SRX Series on page 39](#)

## Understanding Security Zones and Policies for SRX Series

This topic includes the following sections:

- [Zones on page 8](#)
- [Security Policy on page 8](#)

### 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 *Security Zones and Interfaces Feature Guide for Security Devices*.

### Security Policy

---

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service.

If the SRX Series receives a packet that matches those specifications, it performs the action specified in the policy. Actions for traffic matching the specified criteria include permit, deny, reject, log, or count.

Security policies enforce a set of rules for transit traffic, identifying which traffic can pass through the firewall and the actions taken on the traffic as it passes through the firewall.

[Table 6 on page 9](#) provides details of factory default settings for security policies on branch SRX Series devices.

**Table 6: 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 *Security Policies Feature Guide for Security Devices*.

**Related  
Documentation**

- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)
- [Example: Configuring Security Zones and Policies for SRX Series on page 39](#)

## 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 details, see *Network Address Translation Feature Guide for Security Devices*.

**Related  
Documentation**

- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)
- [Example: Configuring Destination NAT for SRX Series on page 43](#)

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

Table 7: 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	
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 48.](#))
- 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 *Junos OS UTM Library for Security Devices*.

#### Related Documentation

- [Updating Licenses for a Branch SRX Series on page 48](#)
- [Example: Configuring Unified Threat Management for a Branch 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 48](#).
- 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.

For more details on IDP, see *Junos OS Intrusion Detection and Prevention (IDP) Library for Security Devices*.

### Related Documentation

- [Updating Licenses for a Branch SRX Series on page 48](#)
- [Example: Configuring Intrusion Detection and Prevention for SRX Series on page 53](#)

## 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

For more information, see *IPsec VPN Feature Guide for Security Devices*.

**Related Documentation**

- *Junos OS VPN Library for Security Devices*

## Understand 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.

For more information, see *Chassis Cluster Feature Guide for Security Devices*.

**Related Documentation**

- *Chassis Cluster Feature Guide for Security Devices*





## CHAPTER 2

# Configuration

- [SRX Series Basics on page 15](#)
- [SRX Series Security on page 38](#)
- [Configuration Statements on page 57](#)

### SRX Series Basics

---

- [Mandatory Settings to Configure Your Branch SRX Series on page 15](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)
- [Connecting Your Branch SRX Series Through the Console Port for the First Time on page 25](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 26](#)
- [Configuring Internet Access for Your Branch SRX Series on page 27](#)
- [Configuring a Network Time Protocol Server for Your Branch SRX Series on page 31](#)
- [Validating Your Branch SRX Series Configuration on page 32](#)
- [Verifying Your Branch SRX Series Configuration on page 33](#)
- [SRX210 Factory Default Setting—A Sample on page 34](#)
- [Resetting Your Branch SRX Series on page 38](#)

### Mandatory Settings to Configure Your Branch SRX Series

[Table 8 on page 15](#) provides the details on configuration settings that you need to enter when configuring the device for the first time.

**Table 8: 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.

**Table 8: Settings Used to Configure the SRX210 (continued)**

Settings	Details
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 <a href="http://tf.nist.gov/tf-cgi/servers.cgi">http://tf.nist.gov/tf-cgi/servers.cgi</a> .
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><b>NOTE:</b> The DHCP client configuration is by default enabled on port 0/0 (ge-0/0/0).</p> <p><b>NOTE:</b> 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 3](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)

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

This topic includes the following sections:

- [Connecting Your Branch SRX Series Through the Console Port for the First Time on page 16](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)
- [Configuring Internet Access for Your Branch SRX Series on page 18](#)
- [Configuring a Network Time Protocol Server for Your Branch SRX Series on page 23](#)
- [Validating Your Branch SRX Series Configuration on page 23](#)
- [Verifying Your Branch SRX Series Configuration on page 24](#)

**Connecting Your 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 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 System Identification and User Classes for Your Branch SRX Series” on page 18](#).



**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>.

---

### Configuring System Identification and User Classes for Your Branch SRX Series

After assigning a root password, you must set up a hostname, domain name, and user accounts. All the users logging in to the SRX Series must be mapped to a login class. You can use the predefined login classes: `operator`, `read-only`, `super-user`, and `unauthorized`, or create a new login class. You can then apply one login class to an individual user account.

To configure system identification settings and user classes:

1. Set the system hostname.

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

2. Create an administrative user to manage the SRX Series.

```
[edit]
root@host# set system login user admin-user class super-user
root@host# set system login user admin-user authentication plain-text-password
```

Enter the password and retype the password when prompted.

3. Create a read-only administrative user.

```
[edit]
root@host# set system login user read-only-user class read-only
root@host# set system login user read-only-user authentication plain-text-password
```

Enter the password and retype the password when prompted.

---

### Configuring Internet Access for Your Branch SRX Series

In this example you create a configuration for connecting your branch SRX Series device to the Internet, allowing users and devices connected to your branch SRX Series device to send and receive traffic to a remote site.



**NOTE:** This procedure applies to most branch SRX Series devices. Any differences might be related to the types of interfaces available on your branch SRX Series device. For example, you might have to substitute `fe-x/x/x` interfaces for `ge-x/x/x` interfaces when configuring this procedure. This procedure uses the SRX210 as example.



**NOTE:** This procedure assumes that the branch SRX Series device still has the factory default zones, policies, and source Network Address Translation (NAT) configuration commands in place. If your branch SRX Series device is unable to connect to the Internet after you have completed the tasks in this document, the information in [“SRX210 Factory Default Setting—A Sample” on page 34](#) might help you diagnose and fix the problem.

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

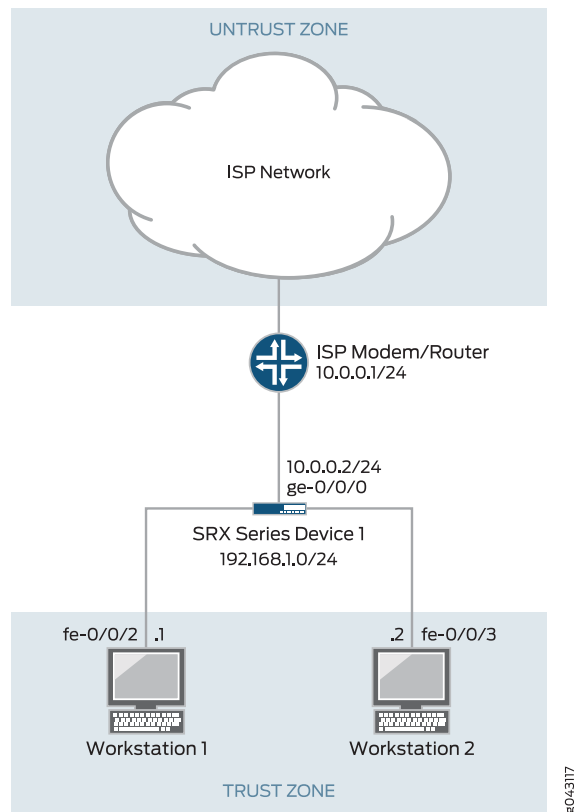
- **Autoinstallation**—The interface ge-0/0/0 (the interface used to connect to your ISP) does not have IP options configured when the SRX Series device is removed from its box and powered on, or you reload the factory default configuration.

Interface ge-0/0/0 is configured with the BOOTP command when you commit the configuration without configuring either DHCP or an IP address on interface ge-0/0/0. When interface ge-0/0/0 is configured to use BOOTP, the SRX Series device attempts to use BOOTP to obtain its configuration from a BOOTP server in the ISP’s network (using BOOTP to download a configuration for any Juniper Networks device is referred to as autoinstallation). When you commit a configuration that was obtained through a BOOTP, the **autoinstallation** command is removed from the configuration of your branch SRX Series device automatically. This method is not explained in this example. For more details on autoinstallation, see [“Autoinstallation Overview” on page 151](#).

- **DHCP**—Assign the Internet connectivity information to the branch SRX Series device automatically using DHCP from the ISP—If your ISP supports DHCP, the branch SRX Series device will acquire an IP address and other settings (a domain name server IP address and a default route) from your ISP automatically. This method is explained in this example.
- **Manually**—Assign the Internet connectivity information to the branch SRX Series device manually—If your ISP does not provide IP address information through DHCP, you can configure the Internet interface with a static IP address, a DNS IP address, and a default route pointing to the ISP’s Internet router. This method is explained in this example.

[Figure 2 on page 20](#) shows how to connect a branch SRX Series device to the Internet.

Figure 2: Connecting a Branch SRX Series Services Gateway to the Internet



To acquire the IP connectivity information for the branch SRX Series device automatically using DHCP from your ISP:

1. Open a terminal session with your branch SRX Series device using either a console port connection or SSH.



**NOTE:** If you have not yet configured a password for the root user account then you can only communicate with the branch SRX Series device through the console port. If you need information on how to configure the console port on your device, see [“Connecting Your Branch SRX Series Through the Console Port for the First Time”](#) on page 16.

2. At the login prompt, log in as root, or another user account with superuser privileges, and enter the password when prompted for it.



**NOTE:** If this is the first time you are using your branch SRX Series device, log in as root (prompt for password does not appear). If you have previously configured a password for the root user account, or created another user account, enter the credentials at the prompt. If you have already configured a system hostname, that name will appear in the prompts.

```
Amnesiac (ttyu0)
login: root
Password:
root@%
```



**NOTE:** If you are unable to log in because you do not know the correct password, a password recovery is required. The password recovery process can be found here: <http://kb.juniper.net/KB12167>.

- At the **root@%** prompt, type the **cli** command and press Enter. The prompt changes to **root>** when you enter CLI operational mode.

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

- At the **root>** prompt, type the **configure** command and press Enter. The prompt changes from **root>** to **root#** when you enter configuration mode.

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

- Delete the Autoinstallation system process. This is required because the Autoinstallation system process and using DHCP to set up the Internet connection on interface ge-0/0/0 cannot coexist in the configuration.

```
[edit]
root# delete system autoinstallation
```

- Configure interface ge-0/0/0 to acquire an IP address, a DNS IP address, and a default route from your ISP using DHCP.

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

- When your ISP assigns the Internet connectivity information using DHCP, the process usually also assigns a DNS IP address.

If your ISP instructed you to enter the DNS IP address manually, configure the IP address of the DNS that your ISP provided you with.

```
[edit]
root# set system name-server 10.45.67.1
```



**NOTE:** The ISP might give you more than one DNS IP address to enter manually.



**NOTE:** The DNS IP addresses 208.67.222.222 and 208.67.222.220 are available as part of the default configuration on a branch SRX Series device. You can leave them in the configuration, or remove them.

To assign an IP address, a DNS IP address, and a default route on the branch SRX Series device manually:

1. Configure interface ge-0/0/0 with the IP address that your ISP provided you with.

[edit]

```
root@host# set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.6/30
```

2. Configure a static default route pointing to the ISP's Internet router with IP address 10.0.0.5 as the next hop.

[edit]

```
root# set routing-options static route 0.0.0.0/0 next-hop 10.0.0.5
```

3. Configure the IP address of the DNS that your ISP provided you with.

[edit]

```
root# set system name-server 10.45.67.1
```



**NOTE:** The ISP might give you more than one DNS IP address to enter manually.



**NOTE:** The DNS IP addresses 208.67.222.222 and 208.67.222.220 are available as part of default configuration on branch SRX Series device. You can leave them in the configuration, or remove them.

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

[edit]

```
root# commit
```

[edit]

```
root# commit
commit complete
```

[edit]

```
root#
```

5. Access <http://www.juniper.net> or any webpage to ensure that you are connected to the Internet. This connectivity ensures that you can pass traffic through the services gateway.



### Configuring a Network Time Protocol Server for Your 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
```

### Validating Your 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;
```

11.11.11.11

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

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

### Verifying Your 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 3](#)
  - [Mandatory Settings to Configure Your Branch SRX Series on page 15](#)

## Connecting Your 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 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 System Identification and User Classes for Your Branch SRX Series” on page 18.



**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 Your Branch SRX Series on page 6](#)
  - [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)

## Configuring System Identification and User Classes for Your Branch SRX Series

After assigning a root password, you must set up a hostname, domain name, and user accounts. All the users logging in to the SRX Series must be mapped to a login class. You can use the predefined login classes: operator, read-only, super-user, and unauthorized, or create a new login class. You can then apply one login class to an individual user account.

To configure system identification settings and user classes:

1. Set the system hostname.

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

2. Create an administrative user to manage the SRX Series.

```
[edit]
root@host# set system login user admin-user class super-user
root@host# set system login user admin-user authentication plain-text-password
```

Enter the password and retype the password when prompted.

3. Create a read-only administrative user.

```
[edit]
root@host# set system login user read-only-user class read-only
root@host# set system login user read-only-user authentication plain-text-password
```

Enter the password and retype the password when prompted.

- Related Documentation**
- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
  - [Connecting Your Branch SRX Series Through the Console Port for the First Time on page 16](#)
  - [Configuring Internet Access for Your Branch SRX Series on page 18](#)

- [Validating Your Branch SRX Series Configuration on page 23](#)
- [Verifying Your Branch SRX Series Configuration on page 24](#)

## Configuring Internet Access for Your Branch SRX Series

In this example you create a configuration for connecting your branch SRX Series device to the Internet, allowing users and devices connected to your branch SRX Series device to send and receive traffic to a remote site.



**NOTE:** This procedure applies to most branch SRX Series devices. Any differences might be related to the types of interfaces available on your branch SRX Series device. For example, you might have to substitute fe-x/x/x interfaces for ge-x/x/x interfaces when configuring this procedure. This procedure uses the SRX210 as example.



**NOTE:** This procedure assumes that the branch SRX Series device still has the factory default zones, policies, and source Network Address Translation (NAT) configuration commands in place. If your branch SRX Series device is unable to connect to the Internet after you have completed the tasks in this document, the information in [“SRX210 Factory Default Setting—A Sample” on page 34](#) might help you diagnose and fix the problem.

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

- **Autoinstallation**—The interface ge-0/0/0 (the interface used to connect to your ISP) does not have IP options configured when the SRX Series device is removed from its box and powered on, or you reload the factory default configuration.

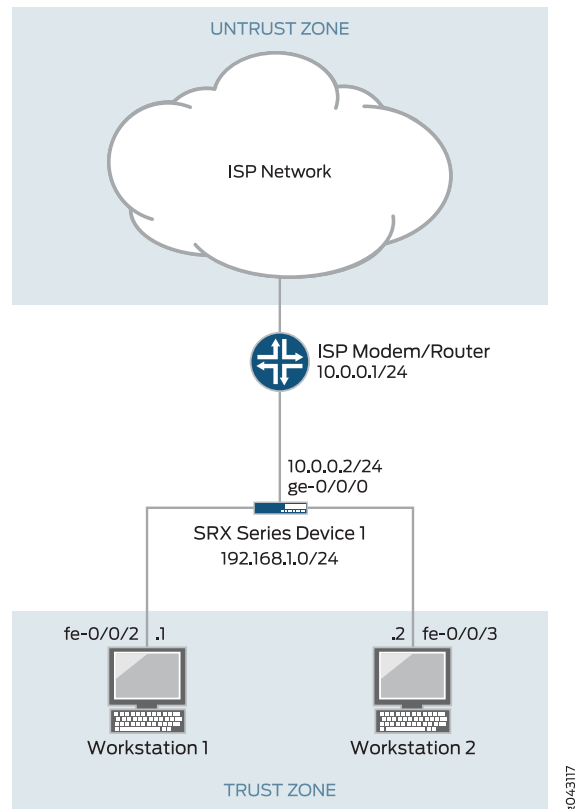
Interface ge-0/0/0 is configured with the BOOTP command when you commit the configuration without configuring either DHCP or an IP address on interface ge-0/0/0. When interface ge-0/0/0 is configured to use BOOTP, the SRX Series device attempts to use BOOTP to obtain its configuration from a BOOTP server in the ISP's network (using BOOTP to download a configuration for any Juniper Networks device is referred to as autoinstallation). When you commit a configuration that was obtained through a BOOTP, the **autoinstallation** command is removed from the configuration of your branch SRX Series device automatically. This method is not explained in this example. For more details on autoinstallation, see [“Autoinstallation Overview” on page 151](#).

- **DHCP**—Assign the Internet connectivity information to the branch SRX Series device automatically using DHCP from the ISP—If your ISP supports DHCP, the branch SRX Series device will acquire an IP address and other settings (a domain name server IP address and a default route) from your ISP automatically. This method is explained in this example.

- Manually—Assign the Internet connectivity information to the branch SRX Series device manually—If your ISP does not provide IP address information through DHCP, you can configure the Internet interface with a static IP address, a DNS IP address, and a default route pointing to the ISP's Internet router. This method is explained in this example.

Figure 2 on page 20 shows how to connect a branch SRX Series device to the Internet.

**Figure 3: Connecting a Branch SRX Series Services Gateway to the Internet**



To acquire the IP connectivity information for the branch SRX Series device automatically using DHCP from your ISP:

1. Open a terminal session with your branch SRX Series device using either a console port connection or SSH.



**NOTE:** If you have not yet configured a password for the root user account then you can only communicate with the branch SRX Series device through the console port. If you need information on how to configure the console port on your device, see “[Connecting Your Branch SRX Series Through the Console Port for the First Time](#)” on page 16.

2. At the login prompt, log in as root, or another user account with superuser privileges, and enter the password when prompted for it.



**NOTE:** If this is the first time you are using your branch SRX Series device, log in as root (prompt for password does not appear). If you have previously configured a password for the root user account, or created another user account, enter the credentials at the prompt. If you have already configured a system hostname, that name will appear in the prompts.

```
Amnesiac (ttyu0)
login: root
Password:
root@%
```



**NOTE:** If you are unable to log in because you do not know the correct password, a password recovery is required. The password recovery process can be found here: <http://kb.juniper.net/KB12167>.

3. At the **root@%** prompt, type the **cli** command and press Enter. The prompt changes to **root>** when you enter CLI operational mode.

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

4. At the **root>** prompt, type the **configure** command and press Enter. The prompt changes from **root>** to **root#** when you enter configuration mode.

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

5. Delete the Autoinstallation system process. This is required because the Autoinstallation system process and using DHCP to set up the Internet connection on interface ge-0/0/0 cannot coexist in the configuration.

[edit]

```
root# delete system autoinstallation
```

6. Configure interface ge-0/0/0 to acquire an IP address, a DNS IP address, and a default route from your ISP using DHCP.

[edit]

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

7. When your ISP assigns the Internet connectivity information using DHCP, the process usually also assigns a DNS IP address.

If your ISP instructed you to enter the DNS IP address manually, configure the IP address of the DNS that your ISP provided you with.

[edit]

```
root# set system name-server 10.45.67.1
```



**NOTE:** The ISP might give you more than one DNS IP address to enter manually.



**NOTE:** The DNS IP addresses 208.67.222.222 and 208.67.222.220 are available as part of the default configuration on a branch SRX Series device. You can leave them in the configuration, or remove them.

To assign an IP address, a DNS IP address, and a default route on the branch SRX Series device manually:

1. Configure interface ge-0/0/0 with the IP address that your ISP provided you with.

[edit]

```
root@host# set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.6/30
```

2. Configure a static default route pointing to the ISP's Internet router with IP address 10.0.0.5 as the next hop.

[edit]

```
root# set routing-options static route 0.0.0.0/0 next-hop 10.0.0.5
```

3. Configure the IP address of the DNS that your ISP provided you with.

[edit]

```
root# set system name-server 10.45.67.1
```



**NOTE:** The ISP might give you more than one DNS IP address to enter manually.





**NOTE:** The DNS IP addresses 208.67.222.222 and 208.67.222.220 are available as part of default configuration on branch SRX Series device. You can leave them in the configuration, or remove them.

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

```
[edit]
root# commit

[edit]
root# commit
commit complete

[edit]
root#
```

5. Access <http://www.juniper.net> or any webpage to ensure that you are connected to the Internet. This connectivity ensures that you can pass traffic through the services gateway.

#### Related Documentation

- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Connecting Your Branch SRX Series Through the Console Port for the First Time on page 16](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)
- [Validating Your Branch SRX Series Configuration on page 23](#)
- [Verifying Your Branch SRX Series Configuration on page 24](#)

## Configuring a Network Time Protocol Server for Your 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 3](#)
- [Connecting Your Branch SRX Series Through the Console Port for the First Time on page 16](#)

- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)
- [Validating Your Branch SRX Series Configuration on page 23](#)
- [Verifying Your Branch SRX Series Configuration on page 24](#)

## Validating Your 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;
11.11.11.11
```

- 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 3](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)
- [Configuring Internet Access for Your Branch SRX Series on page 18](#)

- [Configuring a Network Time Protocol Server for Your Branch SRX Series on page 23](#)
- [Verifying Your Branch SRX Series Configuration on page 24](#)

## Verifying Your 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 3](#)
- [Configuring System Identification and User Classes for Your Branch SRX Series on page 18](#)
- [Configuring Internet Access for Your Branch SRX Series on page 18](#)

- [Configuring a Network Time Protocol Server for Your Branch SRX Series on page 23](#)
- [Validating Your Branch SRX Series Configuration on page 23](#)

## SRX210 Factory Default Setting—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 {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone trust to-zone untrust {
        policy trust-to-untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            vlan.0;
        }
    }
    security-zone untrust {
        screen untrust-screen;
        interfaces {

```

```
ge-0/0/0.0 {  
  host-inbound-traffic {  
    system-services {  
      dhcp;  
      tftp;  
    }  
  }  
}  
}  
}  
}  
}  
}  
}  
vpls {  
  vpls-trust {  
    vpls-id 3;  
    l3-interface vpls.0;  
  }  
}
```

**Related Documentation**

- [Connecting Your Branch SRX Series for the First Time on page 16](#)

## Resetting Your 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 on page 16](#)

---

## SRX Series Security

- [Example: Configuring Security Zones and Policies for SRX Series on page 39](#)
- [Example: Configuring Destination NAT for SRX Series on page 43](#)
- [Updating Licenses for a Branch SRX Series on page 48](#)



- [Example: Configuring Unified Threat Management for a Branch SRX Series on page 50](#)
- [Example: Configuring Intrusion Detection and Prevention for SRX Series on page 53](#)

## Example: Configuring Security Zones and Policies for SRX Series

This example shows how to set up a new zone and add three 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

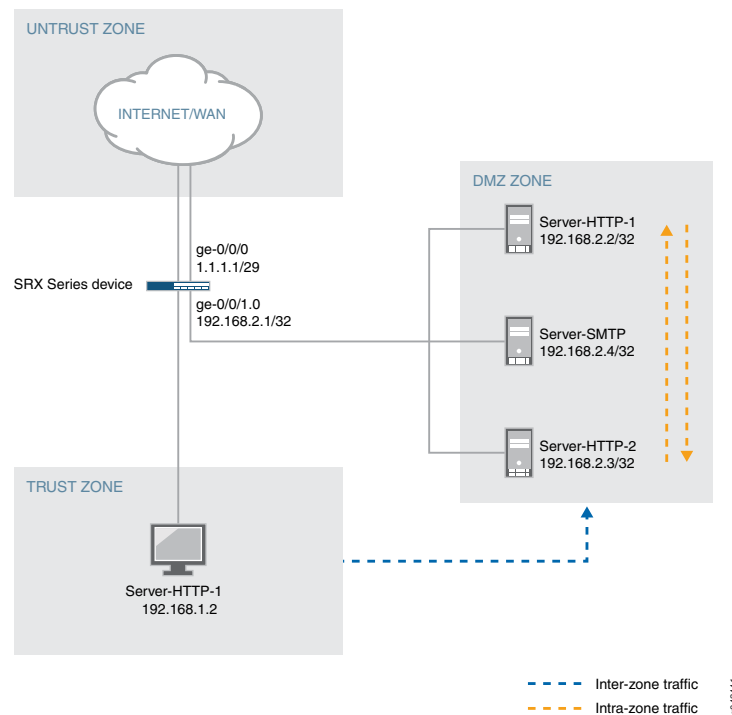
This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

### Overview

This example uses the network topology shown in [Figure 4 on page 39](#).

**Figure 4: 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 9 on page 40](#).

**Table 9: 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 10 on page 40](#).

**Table 10: 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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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 8](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)

## 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 39](#).

This example uses the following hardware and software components:

- An SRX210
- Junos OS Release 12.1X44-D10

### Overview

Using the topology shown in [Figure 5 on page 44](#), 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 11 on page 45](#).

**Figure 5: Destination NAT Single Address Translation**

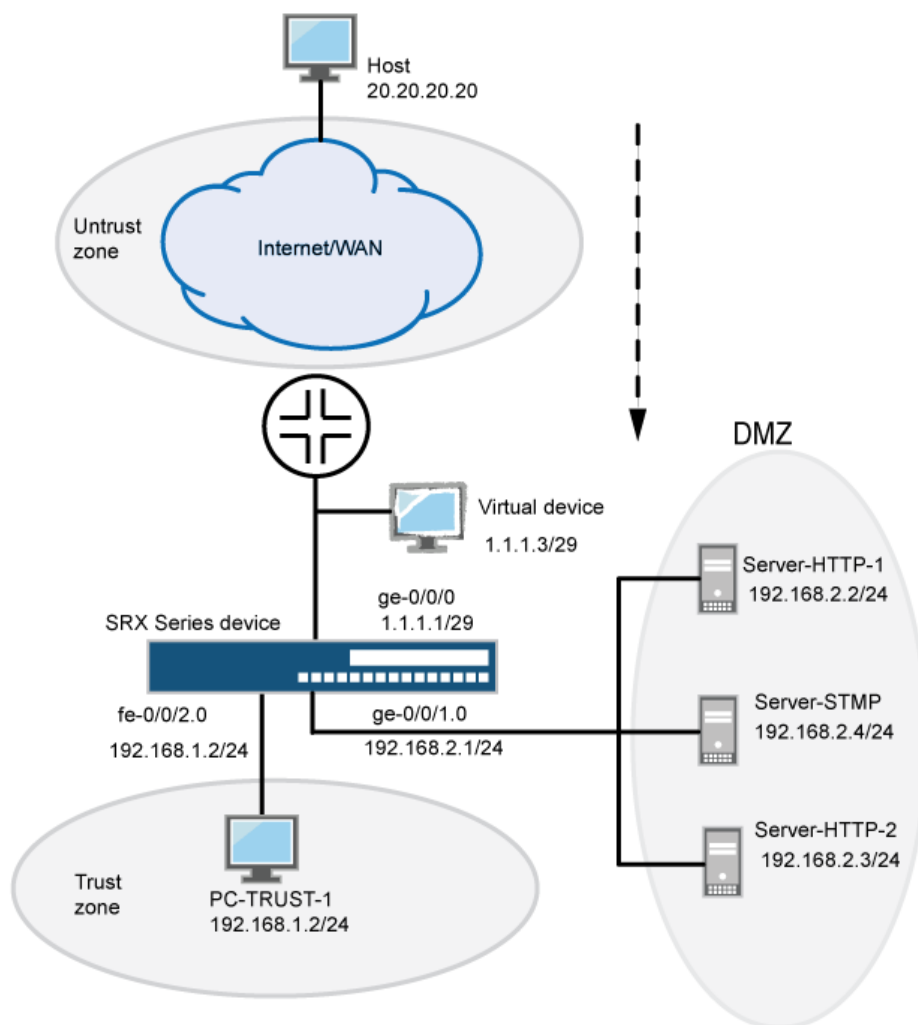


Table 11: Destination NAT Mapping

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, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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 47](#)
- [Verifying NAT Application to Traffic on page 48](#)

### 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-1 192.168.2.2 - 192.168.2.2 Instance 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 9](#)
- [Understanding Factory Default Configuration Settings of an SRX210 on page 3](#)
- [Connecting Your Branch SRX Series for the First Time on page 16](#)

## 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 installed	Licenses used	Expiry 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 98](#)
  - [show system license \(View\) on page 121](#)

## 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 48](#).

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, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
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 52](#)
- [Verifying Antispam Status on page 52](#)
- [Verifying Antivirus Protection on page 52](#)

#### **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 48](#)
  - [Understanding Unified Threat Management for Branch SRX Series on page 10](#)
  - [Predefined UTM Profile Configuration for Branch SRX Series on page 89](#)
  - [Default UTM Policy for Branch SRX Series on page 89](#)

## 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 53](#)
- [Overview on page 53](#)
- [Configuration on page 54](#)
- [Verification on page 56](#)

### 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 48](#).

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 `idp-app-policy-1` to enable IDP services on the traffic flowing on an SRX210. The `idp-app-policy-1` policy directs all traffic flowing from the untrust zone to the previously configured 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 the 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@srx210-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@srx210-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@srx210-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@srx210-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@srx210-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@srx210-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@srx210-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@srx210-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@srx210-host# run request security idp security-package install status
```

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

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

```
[edit]
user@srx210-host# set system scripts commit file templates.xml
```

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@srx210-host# commit
```

12. Display the list of downloaded templates.

```
[edit]
user@srx210-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@srx210-host# set security idp active-policy Recommended
```

14. Confirm the active-policy enabled on your device.

```
[edit]
user@srx210-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.

```
[edit]
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
idp-app-policy-1 match source-address any destination-address any application
any
```

16. Specify the action to be taken on traffic that matches conditions specified in the policy.

```
[edit]
user@srx210-host# set security policies from-zone untrust to-zone DMZ policy
idp-app-policy-1 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 48](#)
- [Understanding Intrusion Detection and Prevention for SRX Series on page 12](#)

## Configuration Statements

---

- [Security Configuration Statement Hierarchy on page 58](#)
- [\[edit security address-book\] Hierarchy Level on page 59](#)
- [\[edit security policies\] Hierarchy Level on page 59](#)
- [\[edit security nat\] Hierarchy Level on page 64](#)
- [\[edit security utm\] Hierarchy Level on page 67](#)
- [\[edit security idp\] Hierarchy Level on page 74](#)
- [\[edit security ike\] Hierarchy Level on page 83](#)
- [\[edit security ipsec\] Hierarchy Level on page 85](#)
- [\[edit security zones\] 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 J Series and 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 59](#)
- [\[edit security alarms\] Hierarchy Level on page 1312](#)
- [\[edit security alg\] 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 752](#)
- [\[edit security datapath-debug\] Hierarchy Level on page 1313](#)
- [\[edit security dynamic-vpn\] 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 74](#)
- [\[edit security ike\] Hierarchy Level on page 83](#)
- [\[edit security ipsec\] Hierarchy Level on page 85](#)
- [\[edit security log\] Hierarchy Level](#)
- [\[edit security nat\] Hierarchy Level on page 64](#)
- [\[edit security pki\] Hierarchy Level](#)
- [\[edit security policies\] Hierarchy Level on page 59](#)
- [\[edit security resource-manager\] Hierarchy Level](#)
- [\[edit security screen\] Hierarchy Level](#)

- [\[edit security softwires\] Hierarchy Level](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 752](#)
- [\[edit security traceoptions\] Hierarchy Level on page 1314](#)
- [\[edit security user-identification\] Hierarchy Level](#)
- [\[edit security utm\] Hierarchy Level on page 67](#)
- [\[edit security zones\] Hierarchy Level on page 87](#)

**Related  
Documentation**

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *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 58](#)
- *MPLS Feature Guide for Security Devices*
- *Address Books and Address Sets Feature Guide for Security Devices*
- *Security Policy Applications Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*

### [\[edit security policies\] 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;
        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;
  }
  source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
  }
  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
        ssl-termination-profile profile-name
    }
    web-authentication {
        client-match user-or-group-name;
    }
}
services-offload;
tcp-options {
    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 58](#)
- [MPLS Feature Guide for Security Devices](#)
- [Application Firewall Feature Guide for Security Devices](#)
- [Application Quality of Service Feature Guide for Security Devices](#)
- [Security Policies Feature Guide for Security Devices](#)
- [Junos OS VPN Library for Security Devices](#)
- [Junos OS Logical Systems Library for Security Devices](#)
- [Unified Access Control Design and Implementation Guide for Security Devices](#)
- [IDP Policies Feature Guide for Security Devices](#)

- *Infranet Authentication Feature Guide for Security Devices*

## [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 {
          (destination-address ip-address | destination-address-name address-name);
          destination-port port-number;
          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-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 (no-translation | port-overloading-factor number | range (port-low | <to
    port-high>));
routing-instance routing-instance-name;
}
pool-default-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 {
            (destination-address <ip-address> | destination-address-name
                <address-name>);
            destination-port port-number;
            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 58](#)
- *Network Address Translation Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Network Monitoring and Troubleshooting Guide for Security Devices*

## [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 58](#)
  - *Junos OS UTM Library for Security Devices*

### [edit security idp] Hierarchy Level

```

security {
  idp {
    active-policy policy-name;
    application-ddos application-name {
      connection-rate-threshold number;
      context context-name {
        exclude-context-values [value];
        hit-rate-threshold number;
        max-context-values number;
        time-binding-count number;
        time-binding-period seconds;
        value-hit-rate-threshold number;
      }
      service service-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;
    }
    nested-application nested-application-name;
    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 {
      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 {

```

```
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;
}
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;
  }
  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;
    }
    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;
    }
    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 {
    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;
    }
    nested-application nested-application-name;
    rpc {
        program-number rpc-program-number;
    }
    tcp {
        minimum-port port-number <maximum-port port-number>;
    }
    udp {
        minimum-port port-number <maximum-port port-number>;
    }
}
regex 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-ddos {
    rule rule-name {
      description text;
      match {
        application (application-name | any | default);
        application-ddos <application-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);
      }
      then {
        action {
          (close-server | drop-connection | drop-packet | no-action);
        }
        ip-action {
          (ip-block | ip-close | ip-connection-rate-limit connections-per-second |
            ip-notify);
          log;
        }
      }
    }
  }
}

```

```
        log-create;
        refresh-timeout;
        timeout seconds;
    }
    notification {
        log-attacks {
            alert;
        }
    }
}
}
}
}
}
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-ddos {
        statistics {
            interval minutes;
        }
    }
    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);
    fifo-max-size value;
    hash-table-size value;
    (log-errors | no-log-errors);
    max-timers-poll-ticks 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);
        (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;
        (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 58](#)
- *IDP Signature Database Feature Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*
- *IDP SSL Inspection Feature Guide for Security Devices*
- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *IDP Class of Service Action Feature Guide for Security Devices*

#### [\[edit security ike\] 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 58](#)
- *MPLS Feature Guide for Security Devices*
- *AutoVPN Feature Guide for SRX Series Gateway Devices*
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*
- *Group VPN Feature Guide for Security Devices*
- *IPsec VPN Feature Guide for Security Devices*
- *Master Administrator for Logical Systems Feature Guide for Security Devices*

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

```

security {
  ipsec {
    internal {
      security-association {
        manual encryption {
          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 58](#)
- *MPLS Feature Guide for Security Devices*
- *AutoVPN Feature Guide for SRX Series Gateway Devices*
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*
- *Group VPN Feature Guide for Security Devices*
- *IPsec VPN Feature Guide for Security Devices*
- *Master Administrator for Logical Systems Feature Guide for Security Devices*

#### [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 58](#)
- *Application Tracking Feature Guide for Security Devices*
- *Security Zones and Interfaces Feature Guide for Security Devices*
- *Junos OS Logical Systems Library for Security Devices*
- *Unified Access Control Design and Implementation Guide for Security Devices*

## CHAPTER 3

# Administration

- [SRX Series Security on page 89](#)
- [Operational Commands on page 96](#)

## SRX Series Security

---

- [Default UTM Policy for Branch SRX Series on page 89](#)
- [Predefined UTM Profile Configuration for Branch SRX Series on page 89](#)

## 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 10](#)
- [Example: Configuring Unified Threat Management for a Branch SRX Series on page 50](#)

## Predefined UTM Profile Configuration for Branch SRX Series

This topic includes the following sections:

- [Antispam on page 90](#)
- [Antivirus on page 90](#)
- [Web Filtering on page 92](#)

## 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 10](#)
  - [Example: Configuring Unified Threat Management for a Branch SRX Series on page 50](#)

---

## Operational Commands

- [request system license update](#)
- [show security idp active-policy](#)
- [show security idp status](#)
- [show security flow session](#)
- [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

---

<b>Syntax</b>	request system license update
<b>Release Information</b>	Command introduced in Junos OS Release 9.5.
<b>Description</b>	Start autoupdating license keys from the LMS server.
<b>Options</b>	<b>trial</b> —Starts autoupdating trial license keys from the LMS server.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <i>UTM Overview Feature Guide for Security Devices</i></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">request system license update on page 98</a> <a href="#">request system license update trial on page 98</a>
<b>Output Fields</b>	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 idp active-policy

<b>Syntax</b>	show security idp active-policy
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display information about the policy name and running detector version with which the policy is compiled from the IDP data plane module.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request security idp security-package download on page 2200</a></li> <li>• <a href="#">request security idp security-package install on page 2202</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Class of Service Action Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp active-policy on page 99</a>
<b>Output Fields</b>	Table 12 on page 99 lists the output fields for the <b>show security idp active-policy</b> command. Output fields are listed in the approximate order in which they appear.

Table 12: 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

<b>Syntax</b>	show security idp status
<b>Release Information</b>	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.
<b>Description</b>	Display the status of the current IDP policy.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp status on page 101</a>
<b>Output Fields</b>	<a href="#">Table 13 on page 100</a> lists the output fields for the <b>show security idp status</b> command. Output fields are listed in the approximate order in which they appear.

**Table 13: 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"> <li>• min—Minimum delay for a packet to receive and return by a node in microseconds.</li> <li>• max—Maximum delay for a packet to receive and return by a node in microseconds.</li> <li>• ave—Average delay for a packet to receive and return by a node in microseconds.</li> </ul>
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, <b>idp-policy-combined</b> is displayed.
Running Detector Version	Current version of the running detector.
Forwarding process mode	IDP dedicated mode: <b>default</b> , <b>equal</b> , <b>idp</b> , or <b>firewall</b> .

## 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 flow session

---

<b>Syntax</b>	<b>show security flow session</b> [ <i>filter</i> ] [brief   extensive   summary ]
<b>Release Information</b>	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.
<b>Description</b>	Display information about all currently active security sessions on the device.
<b>Options</b>	<ul style="list-style-type: none"><li>• <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 <b>show</b> command for examples of the filtered output.  <b>application</b>—Predefined application name  <b>application-firewall</b>—Application firewall enabled  <b>application-firewall-rule-set</b>—Application firewall enabled with the specified rule set  <b>application-traffic-control</b>—Application traffic control rule set name and rule name  <b>destination-port</b>—Destination port  <b>destination-prefix</b>—Destination IP prefix or address  <b>dynamic-application</b>—Dynamic application or nested dynamic application  <b>dynamic-application-group</b>—Dynamic application or nested dynamic application group  <b>encrypted</b>—Encrypted traffic  <b>family</b>—Display session by family  <b>idp</b>—IDP enabled sessions  <b>interface</b>—Name of incoming or outgoing interface  <b>logical-system</b> (<b>all</b>   <i>logical-system-name</i>)—Name of a specific logical system or <b>all</b> to display all logical systems  <b>nat</b>—Display sessions with network address translation  <b>protocol</b>—IP protocol number  <b>resource-manager</b>—Resource manager  <b>session-identifier</b>—Session identifier  <b>source-port</b>—Source port</li></ul>



**source-prefix**—Source IP prefix

**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**

- *Flow-Based Processing Feature Guide for Security Devices*
- *Application Identification Feature Guide for Security Devices*
- *Application Firewall Feature Guide for Security Devices*
- *Application Quality of Service Feature Guide for Security Devices*
- *clear security flow session all*
- *Junos OS Logical Systems Library for Security Devices*

**List of Sample Output**

[show security flow session on page 105](#)  
[show security flow session brief on page 105](#)  
[show security flow session extensive on page 105](#)  
[show security flow session summary on page 106](#)

**Output Fields**

Table 14 on page 103 lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

**Table 14: show security flow session Output Fields**

Field Name	Field Description
<b>Session ID</b>	Number that identifies the session. Use this ID to get more information about the session.
<b>Policy name</b>	Policy that permitted the traffic.
<b>Timeout</b>	Idle timeout after which the session expires.
<b>In</b>	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
<b>Out</b>	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
<b>Total sessions</b>	Total number of sessions.
<b>Status</b>	Session status.
<b>Flag</b>	Internal flag depicting the state of the session, used for debugging purposes.

Table 14: show security flow session Output Fields (*continued*)

Field Name	Field Description
<b>Policy name</b>	Name and ID of the policy that the first packet of the session matched.
<b>Source NAT pool</b>	The name of the source pool where NAT is used.
<b>Dynamic application</b>	Name of the application.
<b>Application traffic control rule-set</b>	AppQoS rule set for this session.
<b>Rule</b>	AppQoS rule for this session.
<b>Forwarding class</b>	The AppQoS forwarding class name for this session that distinguishes the transmission priority
<b>DSCP code point</b>	Differentiated Services (DiffServ) code point (DSCP) value remarked by the matching rule for this session.
<b>Loss priority</b>	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.
<b>Rate limiter client to server</b>	The rate-limiter profile assigned to the client-to-server traffic defining a unique combination of <b>bandwidth-limit</b> and <b>burst-size-limit</b> specifications.
<b>Rate limiter server to client</b>	The rate-limiter profile assigned to the server-to-client traffic defining a unique combination of <b>bandwidth-limit</b> and <b>burst-size-limit</b> specifications.
<b>Maximum timeout</b>	Maximum session timeout.
<b>Current timeout</b>	Remaining time for the session unless traffic exists in the session.
<b>Session State</b>	Session state.
<b>Start time</b>	Time when the session was created, offset from the system start time.
<b>Unicast-sessions</b>	Number of unicast sessions.
<b>Multicast-sessions</b>	Number of multicast sessions.
<b>Failed-sessions</b>	Number of failed sessions.
<b>Sessions-in-use</b>	Number of sessions in use. <ul style="list-style-type: none"> <li>Valid sessions</li> <li>Pending sessions</li> <li>Invalidated sessions</li> <li>Sessions in other states</li> </ul>
<b>Maximum-sessions</b>	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
Flag: 0x40
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 nat destination summary

<b>Syntax</b>	show security nat destination summary <logical-system ( <i>logical-system-name</i>   all)> <root-logical-system>
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. Support for IPv6 logical systems added in Junos OS Release 12.1X45-D10.
<b>Description</b>	Display a summary of Network Address Translation (NAT) destination pool information.
<b>Options</b>	<p><b>none</b>—Display summary information about the destination NAT pool.</p> <p><b>logical-system (<i>logical-system-name</i>   all)</b>—Display summary information about the destination NAT for the specified logical system or for all logical systems.</p> <p><b>root-logical-system</b>—Display summary information about the destination NAT for the master (root) logical system.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>pool (Security Destination NAT)</i></li> <li>• <i>rule (Security Destination NAT)</i></li> <li>• <i>Network Address Translation Feature Guide for Security Devices</i></li> <li>• <i>Junos OS Logical Systems Library for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security nat destination summary on page 108</a>
<b>Output Fields</b>	<a href="#">Table 15 on page 107</a> lists the output fields for the <b>show security nat destination summary</b> 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.

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

Field Name	Field Description
<b>Total destination nat rule number</b>	Number of destination NAT rules.
<b>Total hit times</b>	Number of times a translation in the translation table is used for all the destination NAT rules.
<b>Total fail times</b>	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

<b>Syntax</b>	<pre>show security policies &lt;detail&gt; &lt;none&gt; policy-name <i>policy-name</i> &lt;detail&gt; &lt;global&gt;</pre>
<b>Release Information</b>	<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 <b>Description</b> output field added in Junos OS Release 12.1. Support for negated address added in Junos OS Release 12.1X45-D10.</p>
<b>Description</b>	<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>
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>none</b>—Display basic information about all configured policies.</li> <li>• <b>detail</b>—(Optional) Display a detailed view of all of the policies configured on the device.</li> <li>• <b>policy-name <i>policy-name</i></b>—(Optional) Display information about the specified policy.</li> <li>• <b>global</b>—Display information about global policies.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Ethernet Port Switching Feature Guide for Security Devices</i></li> <li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li> <li>• <i>Infranet Authentication Feature Guide for Security Devices</i></li> <li>• <i>Junos OS UTM Library for Security Devices</i></li> <li>• <i>Security Policies Feature Guide for Security Devices</i></li> <li>• <i>Junos OS Logical Systems Library for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<p><a href="#">show security policies on page 112</a>  <a href="#">show security policies policy-name p1 detail on page 112</a>  <a href="#">show security policies (services-offload) on page 113</a>  <a href="#">show security policies detail on page 114</a>  <a href="#">show security policies policy-name p1 (Negated Address) on page 114</a>  <a href="#">show security policies policy-name p1 detail (Negated Address) on page 115</a></p>
<b>Output Fields</b>	<p><a href="#">Table 16 on page 110</a> lists the output fields for the <b>show security policies</b> command. Output fields are listed in the approximate order in which they appear.</p>

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	<p>Status of the policy:</p> <ul style="list-style-type: none"> <li>• <b>enabled:</b> 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.</li> <li>• <b>disabled:</b> The policy cannot be used in the policy lookup process, and therefore it is not available for access control.</li> </ul>
Index	An 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, and 3. Also, in a from-zoneC-to-zoneD context, four policies might have sequence numbers 1, 2, 3, and 4.
Source addresses	<p>For standard display mode, the names of the source addresses for a policy. Address sets are resolved to their individual names.</p> <p>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.</p>
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"> <li>• <b>IP protocol</b>: The IP protocol used by the application—for example, TCP, UDP, ICMP.</li> <li>• <b>ALG</b>: If an ALG is explicitly associated with the policy, the name of the ALG is displayed. If <b>application-protocol ignore</b> 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 <b>application-protocol ignore</b> is not configured for custom applications.</li> <li>• <b>Inactivity timeout</b>: Elapsed time without activity after which the application is terminated.</li> <li>• <b>Source port range</b>: The low-high source port range for the session application.</li> </ul>
Destination Address Translation	<p>Status of the destination address translation traffic:</p> <ul style="list-style-type: none"> <li>• drop translated—Drop the packets with translated destination addresses.</li> <li>• drop untranslated—Drop the packets without translated destination addresses.</li> </ul>
Application Firewall	<p>An application firewall includes the following:</p> <ul style="list-style-type: none"> <li>• <b>Rule-set</b>—Name of the rule set.</li> <li>• <b>Rule</b>—Name of the rule. <ul style="list-style-type: none"> <li>• <b>Dynamic applications</b>—Name of the applications.</li> <li>• <b>Dynamic application groups</b>—Name of the application groups.</li> <li>• <b>Action</b>—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"> <li>• <b>permit</b></li> <li>• <b>deny</b></li> </ul> </li> </ul> </li> <li>• <b>Default rule</b>—The default rule applied when the identified application is not specified in any rules of the rule set.</li> </ul>
Action or Action-type	<ul style="list-style-type: none"> <li>• The action taken in regard to a packet that matches the policy's tuples. Actions include the following: <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>firewall-authentication</b></li> <li>• <b>tunnel ipsec-vpn <i>vpn-name</i></b></li> <li>• <b>pair-policy <i>pair-policy-name</i></b></li> <li>• <b>source-nat pool <i>pool-name</i></b></li> <li>• <b>pool-set <i>pool-set-name</i></b></li> <li>• <b>interface</b></li> <li>• <b>destination-nat <i>name</i></b></li> <li>• <b>deny</b></li> <li>• <b>reject</b></li> <li>• <b>services-offload</b></li> </ul> </li> </ul>
Session log	<p>Session log entry that indicates whether the <b>at-create</b> and <b>at-close</b> flags were set at configuration time to log session information.</p>

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

Field Name	Field Description
<b>Scheduler name</b>	Name of a preconfigured scheduler whose schedule determines when the policy is active (or inactive) to check an incoming packet to determine how to treat the packet.
<b>Policy statistics</b>	<p>Policy 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>Active sessions</b>—The number of sessions currently present because of access control lookups that used this policy.</li> <li>• <b>Session deletions</b>—The number of sessions deleted since system startup.</li> <li>• <b>Policy lookups</b>—Number of times the policy was accessed to check for a match.</li> </ul> <p><b>NOTE:</b> Configure the Policy P1 with the <b>count</b> option to display policy statistics.</p>

## 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:YMSG
    Dynamic Application groups: junos:web, junos:chat
    Action: deny
  Default rule: permit
Session log: at-create, at-close
Scheduler name: sch20
Policy statistics:
  Input bytes      :          50000          100 bps
  Output bytes     :          40000          100 bps
  Input packets    :           200          200 pps
  Output packets   :           100          100 pps
  Session rate     :             2           1 sps
  Active sessions  :            11
  Session deletions:            20
  Policy lookups   :            12

```

#### 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      :                500                0 bps
    Output bytes     :                408                0 bps
    Input packets    :                 8                0 pps
    Output packets   :                 6                0 pps
    Session rate     :                 3                0 sps
    Active sessions  :                 1
    Session deletions:                 2
    Policy lookups   :                 3
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 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 utm session

---

<b>Syntax</b>	show security utm session
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display general UTM session information including all allocated sessions and active sessions. Also, display information from both nodes in a chassis cluster.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>clear security utm session</i></li><li>• <a href="#">show security utm status on page 117</a></li><li>• <i>Junos OS UTM Library for Security Devices</i></li></ul>
<b>Output Fields</b>	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

---

<b>Syntax</b>	show security utm status
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Support for UTM in chassis cluster added in Junos OS Release 11.4.
<b>Description</b>	Display whether the UTM service is running or not and status of both the nodes (with full chassis cluster support for UTM).
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>clear security utm session</i></li><li>• <a href="#">show security utm session on page 116</a></li><li>• <i>Junos OS UTM Library for Security Devices</i></li></ul>
<b>Output Fields</b>	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

<b>Syntax</b>	<b>show security zones</b> <b>&lt;detail   terse&gt;</b> <b>&lt; zone-name &gt;</b>
<b>Release Information</b>	Command introduced in Junos OS Release 8.5. The <b>Description</b> output field added in Junos OS Release 12.1.
<b>Description</b>	Display information about security zones.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>none</b>—Display information about all zones.</li> <li>• <b>detail   terse</b>—(Optional) Display the specified level of output.</li> <li>• <b>zone-name</b> —(Optional) Display information about the specified zone.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Ethernet Port Switching Feature Guide for Security Devices</i></li> <li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li> <li>• <i>security-zone</i></li> <li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li> <li>• <i>Junos OS Logical Systems Library for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security zones on page 119</a> <a href="#">show security zones abc on page 119</a> <a href="#">show security zones abc detail on page 119</a> <a href="#">show security zones terse on page 120</a>
<b>Output Fields</b>	Table 17 on page 118 lists the output fields for the <b>show security zones</b> 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)

<b>Syntax</b>	show system license <installed   keys   status   usage>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
<b>Description</b>	Display licenses and information about how licenses are used.
<b>Options</b>	<p><b>none</b>—Display all license information.</p> <p><b>installed</b>—(Optional) Display installed licenses only.</p> <p><b>keys</b>—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p><b>status</b>—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p><b>usage</b>—(Optional) Display the state of licensed features.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<p><a href="#">show system license on page 122</a></p> <p><a href="#">show system license installed on page 122</a></p> <p><a href="#">show system license keys on page 123</a></p> <p><a href="#">show system license usage on page 123</a></p> <p><a href="#">show system license status logical-system all on page 123</a></p>
<b>Output Fields</b>	Table 18 on page 121 lists the output fields for the <b>show system license</b> command. Output fields are listed in the approximate order in which they appear.

Table 18: show system license Output Fields

Field Name	Field Description
<b>Feature name</b>	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
<b>Licenses used</b>	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
<b>Licenses installed</b>	Information about the installed license key: <ul style="list-style-type: none"> <li>• <b>License identifier</b>—Identifier associated with a license key.</li> <li>• <b>License version</b>—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.</li> <li>• <b>Valid for device</b>—Device that can use a license key.</li> <li>• <b>Features</b>—Feature associated with a license.</li> </ul>
<b>Licenses needed</b>	Number of licenses required for features being used but not yet properly licensed.
<b>Expiry</b>	Time remaining in the grace period before a license is required for a feature being used.
<b>Logical system license status</b>	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	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

<b>Syntax</b>	<b>show system services dhcp client</b> <b>&lt; <i>interface-name</i> &gt;</b> <b>&lt;statistics&gt;</b>
<b>Release Information</b>	Command introduced in Junos OS Release 8.5.
<b>Description</b>	Display information about DHCP clients.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>none</b>—Display DHCP information for all interfaces.</li> <li>• <b><i>interface-name</i></b> —(Optional) Display DHCP information for the specified interface.</li> <li>• <b>statistics</b>—(Optional) Display DHCP client statistics.</li> </ul>
<b>Required Privilege Level</b>	view and system
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>dhcp (Interfaces)</i></li> <li>• <a href="#">request system services dhcp on page 987</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system services dhcp client on page 125</a> <a href="#">show system services dhcp client ge-0/0/1.0 on page 126</a> <a href="#">show system services dhcp client statistics on page 126</a>
<b>Output Fields</b>	<a href="#">Table 19 on page 124</a> lists the output fields for the <b>show system services dhcp client</b> 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.

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

Field Name	Field Description
DHCP Options	<ul style="list-style-type: none"> <li>• <b>Name:</b> server-identifier, <b>Value:</b> IP address of the name server.</li> <li>• <b>Name:</b> device, <b>Value:</b> IP address of the name device.</li> <li>• <b>Name:</b> domain-name, <b>Value:</b> Name of the domain.</li> </ul>
Packets dropped	Total packets dropped.
Messages received	<p>Number of the following DHCP messages received:</p> <ul style="list-style-type: none"> <li>• <b>DHCPOFFER</b>—First packet received on a logical interface when DHCP is enabled.</li> <li>• <b>DHCPACK</b>—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.</li> <li>• <b>DHCPNAK</b>—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.</li> </ul>
Messages sent	<p>Number of the following DHCP messages sent:</p> <ul style="list-style-type: none"> <li>• <b>DHCPDECLINE</b>—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet.</li> <li>• <b>DHCPDISCOVER</b>—Packet sent on the interface for which the DHCP client is enabled.</li> <li>• <b>DHCPREQUEST</b>—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer.</li> <li>• <b>DHCPINFORM</b>—Packet sent to the DHCP server for local configuration parameters.</li> <li>• <b>DHCPRELEASE</b>—Packet sent to the DHCP server to relinquish network address and cancel remaining lease.</li> <li>• <b>DHCPRENEW</b>—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.</li> <li>• <b>DHCPREBIND</b>—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.</li> </ul>

## 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

- [Overview on page 129](#)
- [Installation on page 163](#)
- [Configuration on page 205](#)
- [Administration on page 253](#)



## CHAPTER 4

# Overview

- [Product Overview on page 129](#)
- [Software Installation and Upgrade on page 135](#)
- [Dual-Root Partitioning and Autorecovery on page 145](#)
- [BIOS Upgrade on page 149](#)
- [Autoinstallation on page 151](#)
- [Licenses on page 156](#)

### Product Overview

---

- [Junos OS Overview on page 129](#)
- [Junos OS Editions on page 130](#)
- [Installation Categories on the J Series Services Routers on page 131](#)
- [Software Naming Convention on page 131](#)
- [Junos OS Release Numbers on page 132](#)
- [Hardware Overview \(J Series Services Routers\) on page 134](#)

### 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. 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 129](#)
- [One Software Release on page 130](#)
- [One Modular Software Architecture on page 130](#)

#### 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 Software Release

---

Each new version of Junos OS is released concurrently for all product lines following a preset quarterly schedule. Furthermore, each new version of 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.

### One Modular Software Architecture

---

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

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

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

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

#### Related Documentation

- [Junos OS Editions on page 130](#)
- *Installation and Upgrade Guide for Security Devices*

## 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.

**Related  
Documentation**

- [Junos OS Overview on page 129](#)
- [Installation Categories on the J Series Services Routers on page 131](#)
- *Installation and Upgrade Guide for Security Devices*

## Installation Categories on the J Series Services Routers

The following installation categories are available with the J Series routers:

- Junos OS, domestic—**junos-jsr-<release>-domestic.tgz**

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

- Junos OS, export—**junos-jsr-<release>-export.tgz**

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

**Related  
Documentation**

- [Junos OS Editions on page 130](#)
- [Junos OS Release Numbers on page 132](#)
- [Software Naming Convention on page 131](#)
- *Installation and Upgrade Guide for Security Devices*

## 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 130](#)
- [Junos OS Release Numbers on page 132](#)
- *Installation and Upgrade Guide for Security Devices*

## 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

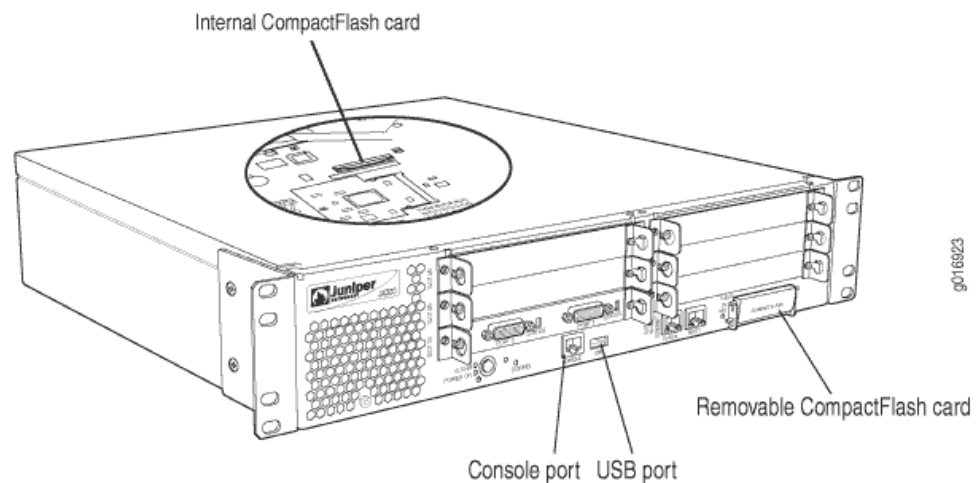
**Related  
Documentation**

- [Junos OS Editions on page 130](#)
- [Software Naming Convention on page 131](#)
- *Installation and Upgrade Guide for Security Devices*

## Hardware Overview (J Series Services Routers)

The Junos OS is installed on the internal CompactFlash card. This internal CompactFlash card is the primary and only boot drive on the J Series routers when they are delivered from the factory. All J Series routers have one or more USB ports. The 4300 and 6300 J Series routers also include an external CompactFlash card slot. You can install external storage devices through the USB ports and CompactFlash card slots. When external storage devices are installed, these external devices can be used as backup boot drives. You can also create a backup internal boot drive on any externally attached CompactFlash card. This CompactFlash card can then be used to replace the internal CompactFlash card on the J Series router in the event that the internal card is damaged or otherwise made unusable by the router. Figure 6 on page 134 shows the location of the memory and ports on a J Series router.

Figure 6: J Series Services Routers (J4300 Shown)



The J Series routers include the following:

- [System Memory on page 134](#)
- [Storage Media on page 135](#)

### System Memory

Starting with Junos OS Release 9.1, all J Series routers require a minimum of 512 MB of router memory on each Routing Engine. Any router without this minimum requires a system memory upgrade before you install Junos OS Release 9.1. To determine the amount of memory currently installed on your router, use the CLI **show chassis routing-engine** command.

For more information about memory requirements for the J Series routers, see the Customer Support Center JTAC Technical Bulletin PSN-2008-04-021:  
<http://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2008-04-021&actionBtn=Search>.



## Storage Media

The J Series routers use the following media storage devices:

- Internal CompactFlash card—The CompactFlash card is the primary boot device.
- External media device—Depending on the system, this external device can be a CompactFlash card or a USB storage device. Juniper Networks recommends that you attach an external device to the system and use this external device as the backup boot device for the system.

[Table 20 on page 135](#) specifies the storage media names used by the J Series routers. The storage media device names are displayed as the router boots.

**Table 20: Routing Engines and Storage Media Names (J Series Routers)**

Routing Engine	Internal CompactFlash Card	External CompactFlash Card J4300 and J6300 Routers Only	USB Storage Media Devices
J Series Routers	ad0	ad2	da0

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

The router attempts to boot from the storage media in the following order:

1. Internal CompactFlash card
2. External CompactFlash card (J4300 and J6300 routers only)
3. USB storage media device

### Related Documentation

- [Junos OS Overview on page 129](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Software Installation and Upgrade

- [Installation Type Overview on page 136](#)
- [Software Package Information Security on page 137](#)
- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Understanding Junos OS Upgrades for J Series Devices on page 138](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices on page 139](#)
- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 140](#)

- [Installation Modules on page 142](#)
- [Understanding Download Manager on page 143](#)

## 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 example, you might upgrade an M120 router running the Junos OS installed using the `jinstall*` installation package. If you upgrade the router from the 9.0R2.10 release to the 9.1R1.8 release, you use the `jinstall-9.1R1.8-domestic-signed.tgz` installation package.

### Category Change Installation

---

The category change installation process is used to move from one category of the Junos OS to another on the same router; for example, moving from a Junos OS standard installation on an M Series, MX Series, or T Series router 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

- [Installation and Upgrade Guide for Security Devices](#)

## 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 136](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding Junos OS Upgrades for SRX Series Devices

SRX Series devices are delivered with Junos OS preinstalled on them. When you power on the 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 your software to use them. Before an upgrade, we recommend that you back up your primary boot device.

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.

### Related Documentation

- [Understanding Junos OS Upgrade and Downgrade Procedures for on SRX Series Devices on page 139](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding Junos OS Upgrades for J Series Devices

J Series devices are delivered with Junos OS preinstalled. When you power on the 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.

On a device, 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, or configure a boot device to receive core dumps for troubleshooting.

If the J 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 CompactFlash (CF) card with either a UNIX or Microsoft Windows computer.



**NOTE:** The terms *Junos OS (legacy services)* and *Junos OS* are used frequently in this section. Junos OS (legacy services) denotes the packet-based software for the J Series device, whereas Junos OS denotes the flow-based software for the J Series device.

### Related Documentation

- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 140](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 175](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Example: Downgrading Junos OS on J Series Devices on page 201](#)
- [Installation and Upgrade Guide for Security Devices](#)

## 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

- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 185](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 199](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding Junos OS Upgrade and Downgrade Procedures for on 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 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.
- **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 137](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 199](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices

Typically, you upgrade Junos OS by downloading a Junos OS 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 Junos OS image, decompresses the image, and installs the decompressed Junos OS. Finally, you reboot the device, at which time it boots from the upgraded Junos OS. Junos OS is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software.

- [Junos OS Upgrade Packages on page 140](#)
- [Junos OS Recovery Packages on page 141](#)

### Junos OS Upgrade Packages

A Junos OS upgrade package name is in the following format:

**package-name-m.nZx-distribution.tgz.**

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n** —Junos OS release, with m representing the major release number and n representing the minor release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **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 example is of a Junos OS upgrade package name:

**junos-jsr-8.5R1.1-domestic.tgz.**

### Junos OS Recovery Packages

Download a Junos OS recovery package, also known as an install media package, to recover a primary CompactFlash (CF) card.

A Junos OS recovery package name is in the following format:

**package-name-m.nZx-export-cfnnn.gz.**

- **package-name**—Name of the package; for example, junos-jsr.
- **m.n** —Junos OS release, with m representing the major release number; for example, 8.5.
- **Z**—Type of Junos OS release. For example, R indicates released software, and B indicates beta-level software.
- **x.y**—Junos OS build number and spin number; for example, 1.1.
- **export**—Export indicates that the Junos OS recovery package is the exported worldwide software package version.
- **cfnnn**—Size of the target CF card in megabytes; for example, cf256. The following CF card sizes are supported:
  - 512 MB
  - 1024 MB



**NOTE:** The CF cards with less than 512 MB of storage capacity are not supported

The following example is of a Junos OS recovery package name:

**junos-jsr-8.5R1.1-export-cf256.gz**

#### Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 175](#)

- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Example: Downgrading Junos OS on J Series Devices on page 201](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Installation Modules

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



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

The following installation module files are available for download:

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

### Related Documentation

- [Installation Type Overview on page 136](#)
- [Installation and Upgrade Guide for Security Devices](#)



## Understanding Download Manager

This topic includes the following sections:

- [Overview on page 143](#)
- [Using Download Manager to Upgrade Junos OS on page 143](#)
- [Handling Errors on page 144](#)
- [Considerations on page 144](#)

### 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 is supported on SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways.

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 144 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 <b>start</b> 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 136](#)
- *Installation and Upgrade Guide for Security Devices*

## Dual-Root Partitioning and Autorecovery

- [Dual-Root Partitioning Scheme Overview on page 145](#)
- [Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information on page 147](#)

### Dual-Root Partitioning Scheme Overview

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 the SRX Series Devices on page 146](#)
- [Important Features of the Dual-Root Partitioning Scheme on page 146](#)

### Boot Media and Boot Partition on the 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 22 on page 146](#) provides information on the storage media available on SRX Series devices.

**Table 22: Storage Media on SRX Series Devices**

SRX Series Devices	Storage Media
SRX100, SRX210, and SRX240	<ul style="list-style-type: none"> <li>• Internal NAND flash (default; always present)</li> <li>• USB storage device (alternate)</li> </ul>
SRX650	<ul style="list-style-type: none"> <li>• Internal CF (default; always present)</li> <li>• External flash card (alternate)</li> <li>• USB storage device (alternate)</li> </ul>

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.

- Related Documentation**
- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
  - [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)
  - [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
  - [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
  - [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
  - *Installation and Upgrade Guide for Security Devices*

## Understanding Integrity Check and Autorecovery of Configuration, Licenses, and Disk Information

- [Overview on page 147](#)
- [How Autorecovery Works on page 147](#)
- [How to Use Autorecovery on page 148](#)
- [Data That Is Backed Up in an Autorecovery on page 148](#)
- [Troubleshooting Alarms on page 148](#)
- [Considerations on page 149](#)

### Overview

---

The autorecovery feature is supported on dual-partitioned SRX100, SRX210, SRX220, SRX240, and SRX650 Services Gateways. 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 23 on page 148 lists types of autorecovery alarms, descriptions, and required actions.

**Table 23: Autorecovery Alarms**

Alarm	Alarm Type	Description	Action Required
Autorecovery information needs to be saved	Minor	This alarm indicates: <ul style="list-style-type: none"> <li>• Unsaved data needs to be saved, or saved data contains problems and another save is required.</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that the system has all required licenses and configuration.</li> <li>• Execute the <b>request system autorecovery state save</b> command.</li> </ul>

Table 23: Autorecovery Alarms (*continued*)

Alarm	Alarm Type	Description	Action Required
Autorecovery has recovered corrupted information	Minor	This alarm indicates: <ul style="list-style-type: none"> <li>• Boot time integrity check failed for certain items; however, the items have been recovered successfully.</li> </ul>	<ul style="list-style-type: none"> <li>• No action is required.</li> <li>• Alarm will be cleared on next bootup.</li> </ul>
Autorecovery was unable to recover data completely	Major	This alarm indicates: <ul style="list-style-type: none"> <li>• Boot time integrity check failed for certain items, which could not be recovered successfully.</li> </ul>	<ul style="list-style-type: none"> <li>• The system might be experiencing a fatal malfunction.</li> </ul>

### 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

- [Installation and Upgrade Guide for Security Devices](#)

## BIOS Upgrade

- [Understanding Auto BIOS Upgrade Using Junos CLI on page 149](#)
- [Understanding Manual BIOS Upgrade Using Junos CLI on page 150](#)

### Understanding Auto BIOS Upgrade Using Junos CLI

The BIOS version listed in the **bios-autoupgrade.conf** file is the minimum supported version. If the current device has a BIOS version earlier than the minimum compatible version, then the auto BIOS upgrade feature upgrades the BIOS automatically to the latest version.

The BIOS upgrades automatically in the following scenarios:

- During Junos OS upgrade through either the J-Web user interface or the CLI (using the **request system software add no-copy no-validate software-image**). In this case, only the active BIOS is upgraded.

- During loader installation using TFTP or USB (using the `install tftp:///software-image` command). In this case, only the active BIOS is upgraded.
- During system boot-up. In this case, both the active BIOS and the backup BIOS are upgraded.

#### Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Understanding Manual BIOS Upgrade Using Junos CLI on page 150](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 253](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding Manual BIOS Upgrade Using Junos CLI

For SRX Series appliances, the BIOS consists of a U-boot and the Junos loader. Additionally, a backup BIOS is supported which includes a backup copy of the U-boot in addition to the active copy from which the system generally boots up.

Table 24 on page 150 lists the CLI commands used for manual BIOS upgrade.

**Table 24: CLI Commands for Manual BIOS Upgrade**

Active BIOS	Backup BIOS
<code>request system firmware upgrade re bios</code>	<code>request system firmware upgrade re bios backup</code>

BIOS upgrade procedure:

#### 1. Install the `jloader-srxsme` package.

1. Copy the `jloader-srxsme` signed package to the device.



**NOTE:** The version of the `jloader-srxsme` package you install must match the version of Junos OS.

2. Install the package using the `request system software add <path to jloader-srxsme package> no-copy no-validate` command.



**NOTE:** Installing the `jloader-srxsme` package places the necessary images under `directory/boot`.

2. Verify that the required images for upgrade are installed. Use the `show system firmware` to verify that the correct BIOS image version is available for upgrade.
3. Upgrade the BIOS (Active and backup) image.



**Active BIOS:**

1. Initiate the upgrade using the **request system firmware upgrade re bios** command.
2. Monitor the upgrade status using the **show system firmware** command.



**NOTE:** The device must be rebooted for the upgraded active BIOS to take effect.

**Backup BIOS:**

1. Initiate the upgrade using the **request system firmware upgrade re bios backup** command.
2. Monitor the upgrade status using the **show system firmware** command.

**Related Documentation**

- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Understanding Auto BIOS Upgrade Using Junos CLI on page 149](#)
- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 253](#)
- *Installation and Upgrade Guide for Security Devices*

## Autoinstallation

---

- [Autoinstallation Overview on page 151](#)
- [Automatic Installation of Configuration Files \(J Series Services Routers and SRX Series Services Gateways\) 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.

This section contains the following topics:

- [Automatic Installation of Configuration Files on page 152](#)
- [Supported Autoinstallation Interfaces and Protocols on page 152](#)
- [Typical Autoinstallation Process on a New Device on page 153](#)

### Automatic Installation of Configuration Files

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

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

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

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

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

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

### Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a device can take place, the device must acquire an IP address. The protocol or protocols you choose for IP address acquisition determine the device interface to connect to the network for autoinstallation. The device detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface or a serial LAN or WAN interface. [Table 25 on page 152](#) lists the protocols that the device can use on these interfaces for IP address acquisition.

**Table 25: 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)

Table 25: Interfaces and Protocols for IP Address Acquisition During Autoinstallation (*continued*)

Interface and Encapsulation Type	Protocol for Autoinstallation
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**

- *Automatic Installation of Configuration Files (J Series Routers and SRX Series Services Gateway)*
- [Example: Configuring Autoinstallation on page 205](#)
- *Installation and Upgrade Guide for Security Devices*

## Automatic Installation of Configuration Files (J Series Services Routers and SRX Series Services Gateways)

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for a device configured for autoinstallation.

### J Series Automatic Installation Overview

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

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

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

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

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

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

## SRX Series Services Gateways Automatic Installation Overview

---

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

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.

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 services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway 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.

### Related Documentation

- [Autoinstallation Overview on page 151](#)
- [Example: Configuring Autoinstallation on page 205](#)
- *Installation and Upgrade Guide for Security Devices*

## Licenses

---

- [Junos OS License Overview on page 156](#)
- [License Enforcement on page 159](#)
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)

### Junos OS License Overview

To enable some Junos OS features, you must purchase, install, and manage separate software licenses. For those features that require a license, the presence on the device of the appropriate software license keys (passwords) determines whether you can use the feature.

For information about how to purchase software licenses for your device, contact your Juniper Networks sales representative.

Certain Junos OS features require licenses. Each license is valid for only a single device. To manage the licenses, you must understand license enforcement and the components of a license key.

This section contains the following topics:

- [License Enforcement on page 157](#)
- [License Key Components on page 157](#)
- [License Management Fields Summary on page 157](#)

### License Enforcement

For features that require a license, you must install and properly configure the license to use the feature. Although the device allows you to commit a configuration that specifies a feature requiring a license when the license is not present, you are prohibited from actually using the feature.

Successful commitment of a configuration does not imply that the required licenses are installed. If a required license is not present, the system provides a warning message after it commits the configuration rather than failing to commit it because of a license violation.

### 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 26 on page 157](#).

**Table 26: Summary of License Management Fields**

Field Name	Definition
<b>Feature Summary</b>	
Feature	<p>Name of the licensed feature:</p> <ul style="list-style-type: none"> <li>• <b>Features</b>—Software feature licenses.</li> <li>• <b>All features</b>—All-inclusive licenses</li> </ul>

Table 26: Summary of License Management Fields (*continued*)

Field Name	Definition
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.
<b>Installed Licenses</b>	
ID	Unique alphanumeric ID of the license.
State	<b>Valid</b> —The installed license key is valid. <b>Invalid</b> —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. <b>NOTE:</b> 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**
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
  - [Generating a License Key on page 254](#)
  - [Updating License Keys on page 256](#)
  - [Saving License Keys on page 255](#)
  - [Downloading License Keys on page 255](#)
  - *Installation and Upgrade Guide for Security Devices*
  - *Administration Guide for Security Devices*



## 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 router or switch enables you to commit a configuration that specifies a licensable feature or scale without a license for a 30-day grace period. The grace period is a short-term grant that enables you to start using features in the pack or scale up to the system limits (regardless of the license key limit) without a license key installed. The grace period begins when the licensable feature or scaling level is actually used by the device (not when it is first committed). In other words, you can commit licensable features or scaling limits to the device configuration, but the grace period does not begin until the device uses the licensable feature or exceeds a licensable scaling level.



**NOTE:** Configurations might include both licensed and nonlicensed features. For these situations, the license is enforced up to the point where the license can be clearly distinguished. For example, an authentication-order configuration is shared by both Authentication, Authorization, and Accounting (AAA), which is licensed, and by Layer 2 Tunneling Protocol (L2TP), which is not licensed. When the configuration is committed, the device does not issue any license warnings, because it is not yet known whether AAA or L2TP is using the configuration. However, at runtime, the device checks for a license when AAA authenticates clients, but does not check when L2TP authenticates clients.

The device reports any license breach as a warning log message whenever a configuration is committed that contains a feature or scale limit usage that requires a license. Following the 30-day grace period, the device periodically reports the breach to syslog messages until a license is installed and properly configured on the device to resolve the breach.



**NOTE:** Successful commitment of a licensable feature or scaling configuration does not imply that the required licenses are installed or not required. If a required license is not present, the system issues a warning message after it commits the configuration.

### Related Documentation

- *Junos OS Feature Licenses*
- *Installation and Upgrade Guide for Security Devices*

## Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 27 on page 160](#) describes the Junos OS features that require licenses.

**Table 27: 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									
UTM	X*	X	X *	X	X *	X	X	X	X	X

\* Indicates support on high-memory devices only.

Each license allows you to run the specified advanced software features on a single device.

**Related Documentation**

- [Junos OS License Overview on page 156](#)
- *Installation and Upgrade Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*

- *Administration Guide for Security Devices*



## CHAPTER 5

# Installation

- [Software Installation and Upgrade on page 163](#)
- [Dual-Root Partitioning and Autorecovery on page 187](#)
- [Boot Loaders and Boot Devices on page 197](#)
- [Software Downgrade on page 199](#)

### Software Installation and Upgrade

---

- [Upgrading Individual Software Packages on page 164](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Preparing the USB Flash Drive to Upgrade Junos OS on page 168](#)
- [Determining the Junos OS Version on page 170](#)
- [Connecting to the Console Port on page 170](#)
- [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 171](#)
- [Downloading Software on page 172](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 174](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 175](#)
- [Checking the Current Configuration and Candidate Software Compatibility on page 175](#)
- [Verifying Available Disk Space on SRX Series Devices on page 176](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Installing Junos OS Using TFTP on SRX Series Devices on page 181](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 185](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 186](#)

## Upgrading Individual Software Packages

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
```

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



**NOTE:** This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.



**NOTE:** Running the `request system snapshot` command overwrites the previous version of the software stored in the backup media.



**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 device, 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:** For high-end SRX Series devices, do not include the *re0 | re1* option when you install a package using the `request system software add` command, if the Routing Engine on which the package is located and the Routing Engine on which you want to install the package is the same. In such cases, the package gets deleted after a successful upgrade.

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
```



**NOTE:** This step is optional for branch SRX Series devices. For branch SRX Series devices, ensure that a USB flash drive is plugged into the USB port of the device.

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



**NOTE:** 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.



**NOTE:** Running the `request system snapshot` command overwrites the previous version of the software stored in backup media.

**Related Documentation**

- *Installation and Upgrade Guide for Security Devices*

## Preparing Your SRX Series Device for Junos OS Upgrades

Before you begin upgrading Junos OS on an SRX Series device, make sure that you have completed the following:

- Obtained 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>.
- Backed up your primary boot device onto a secondary storage device.

Creating a backup has the following advantages:

- If, during an upgrade, the primary boot device fails or becomes corrupted, the device can boot from backup and come back online
- Your active configuration files and log files are retained.
- If an upgrade is unsuccessful, the device can recover using a known, stable environment.

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 28 on page 166](#) lists the secondary storage devices available on an SRX Series devices.

**Table 28: Secondary Storage Devices for SRX Series Devices**

Storage Device	Available on Services Gateways	Minimum Storage Required
USB storage device	SRX100, SRX210, SRX220, and SRX240 Services Gateways	1 GB
	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.

**Related Documentation**

- [Upgrading Individual Software Packages on page 164](#)
- *Installation and Upgrade Guide for Security Devices*
- [Determining the Junos OS Version on page 170](#)
- [Connecting to the Console Port on page 170](#)
- [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 171](#)
- *Installation and Upgrade Guide for Security Devices*

## Preparing Your J Series Services Router for Junos OS Upgrades

Before you begin upgrading Junos OS on J Series devices:

- Obtain a Juniper Networks Web account and a valid support contract. You must have an account to download Junos OS 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.

[Table 29 on page 167](#) lists the secondary storage devices available in a J Series device for backup.

**Table 29: Secondary Storage Devices for Backup**

Storage Device	Available on J Series Devices	Minimum Storage Required
External CompactFlash (CF) card	J2320 and J2350	512 MB

**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, back up the new current configuration to the secondary device.



**NOTE:** Previously, upgrading images on J Series devices with a 256 MB CF card from Junos OS Release 8.5 and earlier involved removing unwanted files in the images and removing the Swap Partition. From Junos OS Release 9.2 and later, as an alternative, Junos OS accomplishes the upgrade efficiently to take another snapshot of the CF card, install the image, and restore configurations.

**Related Documentation**

- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 140](#)
- [Downloading Junos OS Upgrades for J Series Devices on page 175](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Example: Downgrading Junos OS on J Series Devices on page 201](#)
- *Installation and Upgrade Guide for Security Devices*

## Preparing the USB Flash Drive to Upgrade Junos OS



**NOTE:** This topic is applicable only to SRX100, SRX210, SRX220, SRX240, and SRX650 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

- [Upgrading Individual Software Packages on page 164](#)

- *Installation and Upgrade Guide for Security Devices*

## 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

- [Upgrading Individual Software Packages on page 164](#)
- [Connecting to the Console Port on page 170](#)
- [Backing Up the Current Installation \(J Series Services Routers and SRX Series Services Gateways\) on page 171](#)
- *Installation and Upgrade Guide for Security Devices*

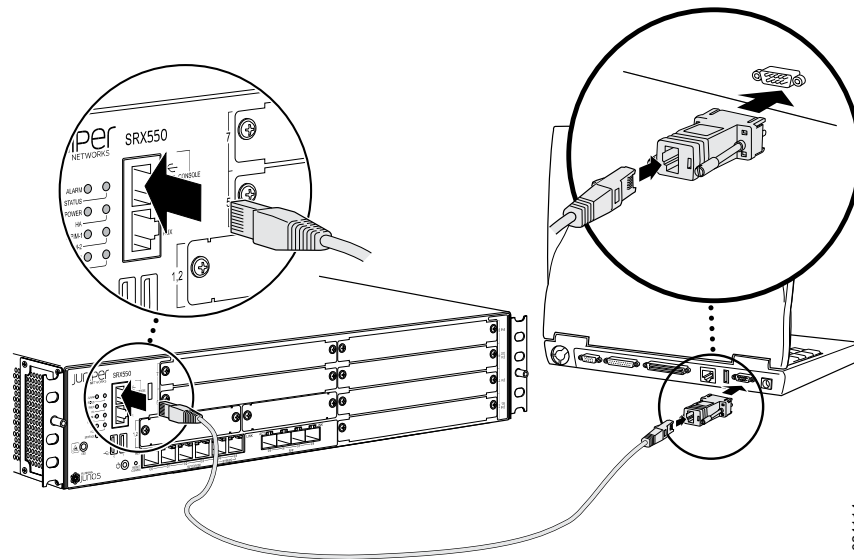
## Connecting to the Console Port

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 7 on page 171](#).

Figure 7: 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

- [Upgrading Individual Software Packages on page 164](#)
- [Determining the Junos OS Version on page 170](#)
- *Installation and Upgrade Guide for Security Devices*

## Backing Up the Current Installation (J Series Services Routers and SRX Series Services Gateways)

You should back up the current installation so that you can return to the current software installation. In a dual Routing Engine system, you need to back up both Routing Engines.

The installation process using the installation package (**junos-jsr\***) removes all stored files on the router 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.

The following instructions offer the minimum steps required to create a backup on a J Series router during the installation process.

To back up the Junos OS on the J Series routers:

1. Attach an external memory device to the router.



**NOTE:** Even when attached to a J Series router, the USB memory device is not listed as a storage device in the `show system storage` CLI command output. You can view the installed USB memory device on the J-Web interface's system monitor screen.

2. Issue the `request system snapshot media usb` command.

The current software installation and configuration are saved on the external USB storage device.

**Related Documentation**

- [Downloading Software on page 172](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 174](#)
- *Installation and Upgrade Guide for Security Devices*

## Downloading Software

You can download the software in one of the two ways:

- [Downloading Software with a Browser on page 172](#)
- [Downloading Software Using the Command-Line Interface on page 173](#)

### 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 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

- [Upgrading Individual Software Packages on page 164](#)
- [Checking the Current Configuration and Candidate Software Compatibility on page 175](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Downloading Junos OS Upgrades for SRX Series Devices

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/csc/swdist-domestic/>
  - <https://www.juniper.net/support/csc/swdist-ww/>
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**
- [Upgrading Individual Software Packages on page 164](#)
  - [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
  - [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Checking the Current Configuration and Candidate Software Compatibility on page 175](#)
  - *Installation and Upgrade Guide for Security Devices*

## Downloading Junos OS Upgrades for J Series Devices

To download software 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 either Canada and U.S. Version or Worldwide Version:
  - <https://www.juniper.net/support/csc/swdist-domestic/>
  - <https://www.juniper.net/support/csc/swdist-ww/>
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select the appropriate software image for your platform.
4. Download the software to a local host or to an internal software distribution site.

- Related Documentation**
- [Understanding Junos OS Upgrade and Downgrade Procedures for J Series Devices on page 140](#)
  - [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
  - [Example: Downgrading Junos OS on J Series Devices on page 201](#)
  - *Installation and Upgrade Guide for Security Devices*

## 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**
- [Downloading Software on page 172](#)
  - *Installation and Upgrade Guide for Security Devices*

## 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@host> 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

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.

#### Related Documentation

- [Downloading Software on page 172](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Example: Installing Junos OS Upgrades on SRX Series Devices

This example shows how to install upgrades on the SRX Series devices.

- [Requirements on page 177](#)
- [Overview on page 178](#)
- [Configuration on page 178](#)
- [Verification on page 179](#)

### Requirements

Before you begin:

- Verify the available space on the internal media. See "[Verifying Available Disk Space on SRX Series Devices](#)" on page 176.

- Download the software package. See “[Downloading Junos OS Upgrades for SRX Series Devices](#)” on page 174.
- 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` 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.
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*.

To install Junos OS upgrades on SRX Series devices:

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.

```
user@host> request system software add /var/tmp/junos-srxsme-10.0R2-domestic.tgz
no-copy no-validate 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

**Purpose** Verify that the Junos OS upgrade was installed.

**Action** From operational mode, enter the `show system` command.

**Related Documentation**

- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 199](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)

## Example: Installing Junos OS Upgrades on J Series Devices

This example shows how to install Junos OS upgrades on J Series devices.

- [Requirements on page 180](#)
- [Overview on page 180](#)
- [Configuration on page 180](#)
- [Verification on page 181](#)

## Requirements

---

Before you begin:

- Verify the available space on the CompactFlash card. See the *Junos OS Release Notes*.
- Download the Junos OS package. See “[Downloading Junos OS Upgrades for J Series Devices](#)” on page 175.
- Copy the software package to the device if you are installing the Junos OS package from a local directory on the device. We recommend that you copy it to the `/var/tmp` directory.

## Overview

---



**NOTE:** This procedure applies only to upgrading from one Junos OS software release to another or from one Junos OS services release to another.

---

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.

For this example, install the `junos-jsr-8.5R1.1.domestic.tgz` software package and copy it to the `/var/tmp` directory. Set the **unlink** option to remove the package at the earliest opportunity so that the device has enough storage capacity to complete the installation, and set the **no-copy** option to specify that the software package is installed but a copy of the package is not saved.

## Configuration

---

### CLI Quick Configuration

To quickly install Junos OS upgrades on J 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 unlink no-copy /var/tmp/junos-jsr-8.5R1.1.domestic.tgz  
request system reboot
```

### GUI Step-by-Step Procedure

To install Junos OS upgrades on J Series devices:

1. In the J-Web user interface, select **Maintain>Software>Upload Package**.
2. On the Upload Package page, in the File to Upload field, type the location of the software package, or click **Browse** to navigate to the location.
3. Select the Reboot If Required check box to have the device reboot automatically when the upgrade is complete.

4. Click **Upload Package**. Junos OS is activated after the device has rebooted.
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*.

To install Junos OS upgrades on J Series devices:

1. From operational mode, install the new package on the device.

```
user@host> request system software add unlink no-copy
/var/tmp/junos-jsr-8.5R1.1.domestic.tgz
```

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*

**Purpose** Verify that the Junos OS upgrade was installed.

**Action** From operational mode, enter the **show system** command.

**Related Documentation**

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Installing Junos OS Upgrades from a Remote Server on J Series Devices on page 186](#)
- [Example: Rebooting J Series Devices on page 263](#)
- [Example: Halting J Series Devices on page 268](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Installing Junos OS Using TFTP on SRX Series Devices

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 30 on page 182](#).

**Table 30: Environment Variables Settings**

Environment Variables	Description
gatewayip	IP address of the gateway device
ipaddr	IP address of the SRX Series device



Table 30: Environment Variables Settings (*continued*)

Environment Variables	Description
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 in the form: `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**

- [Downloading Software on page 172](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 174](#)
- *Installation and Upgrade Guide for Security Devices*

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

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

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

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

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

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

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

3. Remove the USB flash drive.

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



**NOTE:** If an installation error occurs, the LEDs glow 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

- [Downloading Software on page 172](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Downloading Junos OS Upgrades for SRX Series Devices on page 174](#)
- *Installation and Upgrade Guide for Security Devices*

## Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices

You can use the J-Web user interface to install Junos OS packages that are retrieved with FTP or HTTP from the specified location.

Before you begin:

- Verify the available space on the internal media. See [“Verifying Available Disk Space on SRX Series Devices” on page 176](#).
- Download the Junos OS package. See [“Downloading Junos OS Upgrades for SRX Series Devices” on page 174](#).

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 into the fields described in [Table 31 on page 186](#).

Table 31: 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	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	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

- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Downgrading Junos OS on SRX Series Devices on page 199](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Installing Junos OS Upgrades from a Remote Server on J Series Devices

You can use the J-Web 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 CompactFlash (CF) card. See the *Junos OS Release Notes*.
- Download the software package.

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 described in [Table 32 on page 187](#).

**Table 32: Install Remote Summary**

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following:  <i>ftp://hostname/pathname/package-name</i>  <i>http://hostname/pathname/package-name</i>
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	Specifies that the device is automatically rebooted when the upgrade is complete.	Select the check the box if you want the device to reboot automatically when the upgrade is complete.

3. Click **Fetch and Install Package**. Junos OS is activated after the device reboots.

#### Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Example: Rebooting J Series Devices on page 263](#)
- [Example: Halting J Series Devices on page 268](#)
- *Installation and Upgrade Guide for Security Devices*

## Dual-Root Partitioning and Autorecovery

- [Understanding Automatic Recovery of the Primary Junos OS Image with Dual-Root Partitioning on page 188](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)

- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
- [Reinstalling the Single-Root Partition Using request system software add Command on page 196](#)

## 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.**

#### Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Dual-Root Partitioning Scheme Overview on page 145](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- *Installation and Upgrade Guide for Security Devices*

## Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series 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.

#### Related Documentation

- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Dual-Root Partitioning Scheme Overview on page 145](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- *Installation and Upgrade Guide for Security Devices*

## Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning

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.

**Related  
Documentation**

- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
- [Dual-Root Partitioning Scheme Overview on page 145](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
- [Reinstalling the Single-Root Partition Using `request system software add` Command on page 196](#)
- *Installation and Upgrade Guide for Security Devices*

## Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices



**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 Using TFTP on SRX Series Devices” on page 181](#)
- 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 Using a USB Flash Drive on SRX Series Devices” on page 184](#)
- 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

- [Dual-Root Partitioning Scheme Overview on page 145](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
- [Installation and Upgrade Guide for Security Devices](#)

### 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 193](#)
- [Overview on page 193](#)
- [Configuration on page 194](#)
- [Verification on page 196](#)

#### 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*.

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 [“Upgrading the Boot Loader on SRX Series Devices” on page 198](#).
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 196](#)

#### *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 Overview on page 145](#)
- [Junos OS Release 10.0 or Later Upgrades with Dual-Root Partitioning on SRX Series Devices on page 192](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- [Understanding How the Primary Junos OS Image with Dual-Root Partitioning Recovers on SRX Series Devices on page 190](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Reinstalling the Single-Root Partition Using **request system software add** Command

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. An error will be returned if this is attempted.



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

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 Overview on page 145](#)
- [Junos OS Release 9.6 or Earlier Installation on SRX Series Devices with Dual-Root Partitioning on page 191](#)
- [Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Boot Loaders and Boot Devices

- [Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series Device on page 197](#)
- [Upgrading the Boot Loader on SRX Series Devices on page 198](#)

### Installing Junos OS from the Boot Loader Using a USB Storage Device on an SRX Series 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.

- Related Documentation**
- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
  - [Installing Junos OS Upgrades from a Remote Server on the SRX Series Devices on page 185](#)
  - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
  - [Installation and Upgrade Guide for Security Devices](#)

## 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**
- [Understanding Junos OS Upgrades for SRX Series Devices on page 137](#)
  - [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
  - [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
  - [Installation and Upgrade Guide for Security Devices](#)



---

## Software Downgrade

---

- [Example: Downgrading Junos OS on SRX Series Devices on page 199](#)
- [Example: Downgrading Junos OS on J Series Devices on page 201](#)

### Example: Downgrading Junos OS on SRX Series Devices

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

- [Requirements on page 199](#)
- [Overview on page 199](#)
- [Configuration on page 199](#)
- [Verification on page 200](#)

---

#### 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.

---

#### 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**

**Purpose** Verify that the Junos OS downgrade was installed.

**Action** From operational mode, enter the **show system** command.

- Related Documentation**
- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
  - [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
  - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
  - [Example: Rebooting SRX Series Devices on page 262](#)
  - [Installation and Upgrade Guide for Security Devices](#)

## Example: Downgrading Junos OS on J Series Devices

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

- [Requirements on page 201](#)
- [Overview on page 201](#)
- [Configuration on page 201](#)
- [Verification on page 202](#)

### Requirements

No special configuration beyond device initialization is required before configuring this feature.

### Overview



**NOTE:** This procedure applies only to downgrading from one Junos OS software release to another or from one Junos OS services release to another.

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.

### Configuration

**CLI Quick Configuration** To quickly downgrade Junos OS on J 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 J 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:** After you downgrade the software, the previous release is loaded, and you cannot reload the running version of software again. 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 J 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***

**Purpose** Verify that the Junos OS downgrade was installed.

**Action** From operational mode, enter the **show system** command.

- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
  - [Example: Rebooting J Series Devices on page 263](#)
  - [Example: Halting J Series Devices on page 268](#)
  - *Installation and Upgrade Guide for Security Devices*



## CHAPTER 6

# Configuration

- [Autoinstallation on page 205](#)
- [Backup and Snapshot Configuration Files on page 208](#)
- [Boot Loaders and Boot Devices on page 210](#)
- [Configuration Statements on page 215](#)

### Autoinstallation

---

- [Example: Configuring Autoinstallation on page 205](#)

#### Example: Configuring Autoinstallation

This example shows how to configure a device for autoinstallation.

- [Requirements on page 205](#)
- [Overview on page 206](#)
- [Configuration on page 206](#)
- [Verification on page 207](#)

#### 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 709](#).
- Create one of the following configuration files, and store it on a TFTP server in the network:
  - 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 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

<b>Purpose</b>	Verify that the device has been configured for autoinstallation.
<b>Action</b>	From operational mode, enter the <b>show system autoinstallation status</b> 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.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Autoinstallation Overview on page 151</a></li> <li>• <i>Automatic Installation of Configuration Files (J Series Routers and SRX Services Gateway)</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>

## Backup and Snapshot Configuration Files

- [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 208](#)
- [Configuring External CompactFlash on SRX650 Devices on page 209](#)

### Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices

Use the **set system dump-device** command to specify the medium to use for the device to store system software failure memory snapshots. In this way, when the operating system fails, if you have specified a system dump device in the configuration, the operating system preserves a snapshot of the state of the device when it failed.

After you reboot the system, the dump device is checked for a snapshot as part of the operating system boot process. If a snapshot is found, it is written to the crash dump directory on the device (**/var/crash**). The customer support team can examine this memory snapshot to help determine the cause of the system software failure.



**NOTE:** If the swap partition on the dump device medium is not large enough for a system memory snapshot, either a partial snapshot or no snapshot is written into the crash dump directory.

From operational mode, enter the **set system dump-device** command with the following syntax:

```
user@host> set system dump-device boot-device | compact-flash |
removable-compact-flash | usb
```

[Table 33 on page 208](#) describes the **set system dump-device** command options.

**Table 33: CLI set system dump-device Command Options**

Option	Description
<b>boot-device</b>	Uses whatever device was booted from as the system software failure memory snapshot device.
<b>compact-flash</b>	Uses the internal CompactFlash (CF) card as the system software failure memory snapshot device.
<b>removable-compact-flash</b>	Uses the CF card on the rear of the device (J2320 and J2350 only) as the system software failure memory snapshot device.
<b>usb</b>	Uses the device attached to the USB port as the system software failure memory snapshot device.

#### Related Documentation

- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Example: Configuring Boot Devices for J Series Devices on page 213](#)

- [Example: Rebooting J Series Devices on page 263](#)
- [Example: Halting J Series Devices on page 268](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Configuring External CompactFlash on SRX650 Devices

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 137](#)
- [Preparing Your SRX Series Device for Junos OS Upgrades on page 166](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Installing Junos OS Using a USB Flash Drive on SRX Series Devices on page 184](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Boot Loaders and Boot Devices

---

- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
- [Example: Configuring Boot Devices for J Series Devices on page 213](#)

### Example: Configuring Boot Devices for SRX Series Devices

This example shows how to configure a boot device.

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

#### 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 166](#).

#### 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*

**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**

- [Upgrading the Boot Loader on SRX Series Devices on page 198](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Rebooting SRX Series Devices on page 262](#)
- [Installation and Upgrade Guide for Security Devices](#)

## Example: Configuring Boot Devices for J Series Devices

This example shows how to configure a boot device.

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

### Requirements

Before you begin, ensure that the backup device has a storage capacity of at least 256 MB. See “[Preparing Your J Series Services Router for Junos OS Upgrades](#)” on [page 167](#).

### Overview

You can configure a boot device to replace the primary boot device on your J 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 J 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 CF card from a special software image. 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.
- After a boot device is created with the default factory configuration, it can operate only in an internal CF slot.
- After the boot device is created as an internal CF, it can operate only in an internal CF slot.

This example configures a boot device to copy the software snapshot to the device connected to the USB port.

### 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 media usb
```

**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, in the Target Media field, specify **usb** as the boot device to copy the snapshot to.
3. Click **Snapshot**.
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 configure a boot device:

From operational mode, create a boot device on an alternate medium to replace the primary boot device or to serve as a backup.

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

**Results**

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

For USB:

```
user@host> show system snapshot media usb
```

```
Information for snapshot on      usb (/dev/dals1a) (primary)
  Creation date: Jul 24 16:16:01 2009
  JUNOS version on snapshot:
  junos   : 10.0I20090723_1017-domestic
Information for snapshot on      usb (/dev/dals2a) (backup)
  Creation date: Jul 24 16:17:13 2009
  JUNOS version on snapshot:
  junos   : 10.0I20090724_0719-domestic
```

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

---

**Verification**

Confirm that the configuration is working properly.

**Verifying the Snapshot Information****Purpose**

Verify that the snapshot information was configured.

**Action**

From operational mode, enter the **show system snapshot media** command.



- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Configuring a Boot Device to Receive Junos OS Failure Memory Snapshots in J Series Devices on page 208](#)
  - [Example: Rebooting J Series Devices on page 263](#)
  - [Example: Halting J Series Devices on page 268](#)
  - *Installation and Upgrade Guide for Security Devices*

## Configuration Statements

- [System Configuration Statement Hierarchy on page 215](#)
- [autoinstallation on page 246](#)
- [configuration-servers on page 247](#)
- [interfaces \(Autoinstallation\) on page 248](#)
- [license on page 249](#)
- [usb on page 251](#)

## 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 J Series and 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];
do-not-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;
}
}
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;
}
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 {  
                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**

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *Firewall User Authentication Feature Guide for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*

## autoinstallation

---

**Syntax**

```
autoinstallation {
  configuration-servers {
    url {
      password password;
    }
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
  usb {
    disable;
  }
}
```

**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.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Autoinstallation on page 205](#)
- *Installation and Upgrade Guide for Security Devices*



## configuration-servers

<b>Syntax</b>	<pre>configuration-servers {     url {         password <i>password</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit system autoinstallation]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<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"> <li>• tftp://hostname/path/filename</li> <li>• ftp://username:password@ftp.hostname.net</li> <li>• http://hostname/path/filename</li> <li>• http://username:password@httpconfig.sp.com</li> </ul>
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>url</b>—Specify the URL address of the server containing the configuration files.</li> <li>• <b>password</b>—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.</li> </ul>
<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>Installation and Upgrade Guide for Security Devices</i></li> </ul>

## interfaces (Autoinstallation)

---

<b>Syntax</b>	<pre>interfaces {     <i>interface-name</i> {         bootp;         rarp;     } }</pre>
<b>Hierarchy Level</b>	[edit system autoinstallation]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	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.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>bootp</b>—Enables BOOTP or DHCP during autoinstallation.</li><li>• <b>rarp</b>—Enables RARP during autoinstallation.</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="#">Example: Configuring Autoinstallation on page 205</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>

## license

<b>Syntax</b>	<pre> license {   autoupdate {     url <i>url</i>;     password <i>password</i>;   }   renew {     before-expiration <i>number</i>;     interval <i>interval-hours</i>;   }   traceoptions {     file {       <i>filename</i> ;       files <i>number</i>;       match <i>regular-expression</i>;       size <i>maximum-file-size</i>;       (world-readable   no-world-readable);     }     flag <i>flag</i>;     no-remote-trace;   } } </pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify license information for the device.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>autoupdate</b>—Autoupdate license keys from license servers. <ul style="list-style-type: none"> <li>• <b>url</b>—URL of a license server.</li> </ul> </li> <li>• <b>renew</b>—License renewal lead time and checking interval. <ul style="list-style-type: none"> <li>• <b>before-expiration <i>number</i></b>—License renewal lead time before expiration in days. <b>Range</b> : 0 through 60 days</li> <li>• <b>interval <i>interval-hours</i></b>—License checking interval in hours. <b>Range</b> : 1 through 336 hours</li> </ul> </li> <li>• <b>traceoptions</b>—Set the trace options. <ul style="list-style-type: none"> <li>• <b>file</b>—Configure the trace file information. <ul style="list-style-type: none"> <li>• <b><i>filename</i></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 <i>number</i></b>— Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</li> </ul> </li> </ul> </li> </ul>

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.

<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 License Overview on page 156</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>
------------------------------	--

---

## usb

---

<b>Syntax</b>	<pre>usb {   disable; }</pre>
<b>Hierarchy Level</b>	[edit system autoinstallation]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Disable the USB autoinstallation process.
<b>Options</b>	<b>disable</b> —Disable the process.
<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="#">Example: Configuring Autoinstallation on page 205</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>



## CHAPTER 7

# Administration

- [Auto BIOS on page 253](#)
- [Licenses on page 253](#)
- [Software Stop and Restart on page 261](#)
- [Operational Commands on page 271](#)

## Auto BIOS

---

- [Disabling Auto BIOS Upgrade on SRX Series Devices on page 253](#)

### 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 137](#)
- [Understanding Auto BIOS Upgrade Using Junos CLI on page 149](#)
- *Installation and Upgrade Guide for Security Devices*

## Licenses

---

- [Displaying License Keys on page 254](#)
- [Generating a License Key on page 254](#)
- [Downloading License Keys on page 255](#)
- [Saving License Keys on page 255](#)

- [Updating License Keys on page 256](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)

## Displaying License Keys

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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

## 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**
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
  - [Updating License Keys on page 256](#)
  - [Saving License Keys on page 255](#)
  - [Displaying License Keys on page 254](#)
  - [Downloading License Keys on page 255](#)
  - [Example: Adding a New License Key on page 257](#)
  - [Example: Deleting a License Key on page 260](#)
  - *Installation and Upgrade Guide for Security Devices*

## 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
  - [Generating a License Key on page 254](#)
  - [Updating License Keys on page 256](#)
  - [Saving License Keys on page 255](#)
  - [Displaying License Keys on page 254](#)
  - [Example: Adding a New License Key on page 257](#)
  - [Example: Deleting a License Key on page 260](#)
  - *Installation and Upgrade Guide for Security Devices*

## 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- [Installation and Upgrade Guide for Security Devices](#)

## 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)

- *Installation and Upgrade Guide for Security Devices*

## Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 257](#)
- [Overview on page 257](#)
- [Configuration on page 257](#)
- [Verification on page 259](#)

### 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: G03000002223
```

```
License version: 2
```

```
Valid for device: JN001875AB
```

Features:

```
  bgp-reflection  - Border Gateway Protocol route reflection
permanent
```

```
License identifier: G03000002225
```

```
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 259](#)
- [Verifying License Usage on page 259](#)
- [Verifying Installed License Keys on page 259](#)

#### *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 xxx
```

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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)

- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*

## Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 260](#)
- [Overview on page 260](#)
- [Configuration on page 260](#)
- [Verification on page 261](#)

---

### 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 G03000002223.

---

### 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 G03000002223
```

#### 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 G03000002223
```



**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****Purpose**

Verify that the expected licenses have been removed from the device.

**Action**

From operational mode, enter the **show system license** command.

**Related Documentation**

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Installation and Upgrade Guide for Security Devices](#)

**Software Stop and Restart**

- [Example: Rebooting SRX Series Devices on page 262](#)
- [Example: Rebooting J Series Devices on page 263](#)
- [Restarting the Chassis on SRX Series Devices on page 265](#)

- [Restarting the Chassis on J Series Devices on page 266](#)
- [Example: Halting SRX Series Devices on page 266](#)
- [Example: Halting J Series Devices on page 268](#)
- [Bringing Chassis Components Online and Offline on SRX Series Devices on page 270](#)
- [Bringing Chassis Components Online and Offline on J Series Devices on page 271](#)

## Example: Rebooting SRX Series Devices

This example shows how to reboot a device.

- [Requirements on page 262](#)
- [Overview on page 262](#)
- [Configuration on page 262](#)
- [Verification on page 263](#)

---

### 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** 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*.

To reboot a device:

From operational mode, schedule a reboot of the SRX Series 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.

```
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

#### Purpose

Verify that the device rebooted.

#### Action

From operational mode, enter the **show system** command.

#### Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Example: Halting SRX Series Devices on page 266](#)
- [Installation and Upgrade Guide for Security Devices](#)

### Example: Rebooting J Series Devices

This example shows how to reboot a J Series device.

- [Requirements on page 264](#)
- [Overview on page 264](#)

- [Configuration on page 264](#)
- [Verification on page 265](#)

---

## 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 USB media while sending a text message of 'stop' to all system users before the device reboots.

---

## Configuration

### CLI Quick Configuration

To quickly reboot a J Series 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 usb message stop
```

### GUI Step-by-Step Procedure

To reboot a J Series 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 **usb** 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*.

To reboot a J Series device:

From operational mode, schedule a reboot of the J Series device to occur fifty minutes from when you set the time from the USB media while sending a text message of 'stop' to all system users before the device reboots.

```
user@host> request system reboot at 5 in 50 media usb 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

**Purpose** Verify that the device rebooted.

**Action** From operational mode, enter the **show system** command.

- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
  - [Example: Downgrading Junos OS on J Series Devices on page 201](#)
  - [Example: Halting J Series Devices on page 268](#)
  - [Installation and Upgrade Guide for Security Devices](#)

## 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
```

- Related Documentation**
- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
  - [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
  - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
  - [Upgrading the Boot Loader on SRX Series Devices on page 198](#)
  - *Installation and Upgrade Guide for Security Devices*

## Restarting the Chassis on J Series Devices

You can restart the chassis using the **restart chassis-control** command with the following options:

- To restart the process.  
`user@host> restart chassis-control |`
- 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`

- Related Documentation**
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
  - [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
  - [Bringing Chassis Components Online and Offline on J Series Devices on page 271](#)
  - [Example: Rebooting J Series Devices on page 263](#)
  - *Installation and Upgrade Guide for Security Devices*

## Example: Halting SRX Series Devices

This example shows how to halt a device.

- [Requirements on page 266](#)
- [Overview on page 267](#)
- [Configuration on page 267](#)
- [Verification on page 268](#)

### 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*.

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*

**Purpose** Verify that the device halted.

**Action** From operational mode, enter the **show system** command.

- Related Documentation**
- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
  - [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
  - [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
  - [Bringing Chassis Components Online and Offline on SRX Series Devices on page 270](#)
  - *Installation and Upgrade Guide for Security Devices*

## Example: Halting J Series Devices

This example shows how to halt a J Series device.

- [Requirements on page 268](#)
- [Overview on page 268](#)
- [Configuration on page 269](#)
- [Verification on page 269](#)

---

### 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 J Series 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 halt at now
```

#### GUI Step-by-Step Procedure

To halt a J Series 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*.

To halt a device:

From operational mode, halt the J 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

#### Purpose

Verify that the device halted.

#### Action

From operational mode, enter the **show system** command.

**Related Documentation**

- [Understanding Junos OS Upgrades for J Series Devices on page 138](#)
- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Example: Downgrading Junos OS on J Series Devices on page 201](#)
- [Example: Rebooting J Series Devices on page 263](#)
- [Installation and Upgrade Guide for Security Devices](#)

**Bringing Chassis Components Online and Offline on SRX Series Devices**

You can use the **request** commands to bring chassis components online and offline.

To bring chassis components online and offline, enter these **request chassis** commands:

```
user@host> request chassis <fru> slot <slot#> pic <pic#> online
```

```
user@host> request chassis <fru> slot <slot#> pic <pic#> offline
```

Where **<fru>** in the request chassis command can be any of the following (for Branch SRX Series devices):

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

Where **<fru>** in the request chassis command can be any of the following (for High-End SRX Series devices):

- **cb**—Changes the control board status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine**—Changes the routing engine status.



**NOTE:** The **request chassis** command is not supported for bringing SPCs online and offline.



**NOTE:** On SRX3000 Series devices, the Network Processing I/O card (NP-IOC) is not hot-swappable and the **request chassis** command is not supported for bringing NP-IOC online and offline. You must power off the services gateway before removing or installing the cards.

Example:

To bring specific pic and the corresponding fpc slot online, from operational mode enter the following **request chassis** command:



```
user@host> request chassis pic pic-slot 1 fpc-slot 1 online
```

#### Related Documentation

- [Example: Configuring Boot Devices for SRX Series Devices on page 210](#)
- [Junos OS Upgrade Methods on the SRX Series Devices on page 138](#)
- [Example: Installing Junos OS Upgrades on SRX Series Devices on page 177](#)
- [Restarting the Chassis on SRX Series Devices on page 265](#)
- *Installation and Upgrade Guide for Security Devices*

## Bringing Chassis Components Online and Offline on J 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:

- **cb**—Changes the control board status.
- **cluster**—Changes the chassis cluster status.
- **fabric**—Changes the fabric status.
- **fpc**—Changes the Flexible PIC Concentrator (FPC) status.
- **fpm**—Changes the craft interface status.
- **pic**—Changes the physical interface card status.
- **routing-engine**—Changes the routing engine status.

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
```

#### Related Documentation


- [Preparing Your J Series Services Router for Junos OS Upgrades on page 167](#)
- [Example: Installing Junos OS Upgrades on J Series Devices on page 179](#)
- [Restarting the Chassis on J Series Devices on page 266](#)
- [Example: Rebooting J Series Devices on page 263](#)
- *Installation and Upgrade Guide for Security Devices*

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

## request system autorecovery state

<b>Syntax</b>	request system autorecovery state (save   recover   clear)
<b>Release Information</b>	Command introduced in Junos Release 11.2.
<b>Description</b>	Prepares the system for autorecovery of configuration, licenses, and disk information.
<b>Options</b>	<p><b>save</b>—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><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.</li> <li>A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.</li> </ul> </div>
	<p><b>recover</b>—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><b>clear</b>—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>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show system autorecovery state on page 292</a></li> <li><i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system autorecovery state save on page 274</a> <a href="#">request system autorecovery state recover on page 274</a> <a href="#">request system autorecovery state clear on page 274</a>
<b>Output Fields</b>	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

<b>Syntax</b>	<code>request system download abort &lt;download-id&gt;</code>
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	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 <b>show</b> command until a Clear operation is performed.
<div>  <b>NOTE:</b> Only downloads in the active, paused, and error states can be aborted. </div>	
<b>Options</b>	<b>download-id</b> —(Required) The ID number of the download to be paused.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system download start on page 279</a></li> <li>• <a href="#">request system download pause on page 277</a></li> <li>• <a href="#">request system download resume on page 278</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system download abort on page 275</a>
<b>Output Fields</b>	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

---


<b>Syntax</b>	request system download clear
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Delete the history of completed and aborted downloads.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">request system download start on page 279</a></li><li>• <a href="#">request system download pause on page 277</a></li><li>• <a href="#">request system download resume on page 278</a></li><li>• <a href="#">request system download abort on page 275</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">request system download clear on page 276</a>
<b>Output Fields</b>	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


<b>Syntax</b>	request system download pause <download-id>
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Suspend a particular download instance.
<div>  <b>NOTE:</b> Only downloads in the active state can be paused.         </div>	
<b>Options</b>	download-id—(Required) The ID number of the download to be paused.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system download start on page 279</a></li> <li>• <a href="#">request system download resume on page 278</a></li> <li>• <a href="#">request system download abort on page 275</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system download pause on page 277</a>
<b>Output Fields</b>	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

<b>Syntax</b>	<code>request system download resume <i>download-id</i> &lt;max-rate&gt;</code>
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	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 <b>request system download start</b> command. The user can optionally specify a new (maximum) bandwidth with the <b>request system download resume</b> command.
<div>  <b>NOTE:</b> Only downloads in the paused and error states can be resumed. </div>	
<b>Options</b>	<p><b>download-id</b>—(Required) The ID number of the download to be paused.</p> <p><b>max-rate</b>—(Optional) The maximum bandwidth for the download.</p>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system download start on page 279</a></li> <li>• <a href="#">request system download pause on page 277</a></li> <li>• <a href="#">request system download abort on page 275</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system download resume on page 278</a>
<b>Output Fields</b>	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

<b>Syntax</b>	<code>request system download start (url   max-rate   save as   login   delay)</code>
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Creates a new download instance and identifies it with a unique integer called the download ID.
<b>Options</b>	<p><b>url</b>—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p><b>max-rate</b>—(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><b>save-as</b>—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p><b>login</b>—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p><b>delay</b>—(Optional) The number of hours after which the download should start.</p>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system download pause on page 277</a></li> <li>• <a href="#">request system download resume on page 278</a></li> <li>• <a href="#">request system download abort on page 275</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system download start on page 279</a>
<b>Output Fields</b>	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

<b>Syntax</b>	request system firmware upgrade
<b>Release Information</b>	Command introduced in Release 10.2 of Junos OS.
<b>Description</b>	Upgrade firmware on a system.
<b>Options</b>	<p><b>fpc</b>—Upgrade FPC ROM monitor.</p> <p><b>pic</b>—Upgrade PIC firmware.</p> <p><b>re</b>—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p><b>vcpu</b>—Upgrade VCPU ROM monitor.</p>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Installation and Upgrade Guide for Security Devices</i></li> <li><i>Administration Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system firmware upgrade on page 280</a>
<b>Output Fields</b>	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 license update

---

<b>Syntax</b>	request system license update
<b>Release Information</b>	Command introduced in Junos OS Release 9.5.
<b>Description</b>	Start autoupdating license keys from the LMS server.
<b>Options</b>	<b>trial</b> —Starts autoupdating trial license keys from the LMS server.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>UTM Overview Feature Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system license update on page 281</a> <a href="#">request system license update trial on page 281</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request system license update

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

```
Request to automatically update license keys from https://ae1.juniper.net has
been sent, use show system license to check status.
```

#### request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net
has been sent, use show system license to check status.
```

## request system partition compact-flash

---

<b>Syntax</b>	request system partition compact-flash
<b>Release Information</b>	Command introduced in Release 9.2 of Junos OS.
<b>Description</b>	Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">request system partition compact-flash (If Yes) on page 282</a> <a href="#">request system partition compact-flash (If No) on page 282</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request system partition compact-flash (If Yes)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>
```

### Sample Output

#### request system partition compact-flash (If No)

```
user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no
```

## request system power-off fpc

<b>Syntax</b>	<code>request system (halt   power-off   reboot) power-off fpc</code>
<b>Release Information</b>	Command introduced in Junos OS Release 11.4.
<b>Description</b>	Bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>halt</b>—Bring FPC offline and then halt the system.</li> <li>• <b>power-off</b>—Bring FPC offline and then power off the system.</li> <li>• <b>reboot</b>—Bring FPC offline and then reboot the system.</li> </ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system halt power-off fpc on page 283</a> <a href="#">request system power-off power-off fpc on page 283</a> <a href="#">request system reboot power-off fpc on page 283</a>
<b>Output Fields</b>	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 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 Release 10.2 of Junos OS.

**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 193](#)
- *Installation and Upgrade Guide for Security Devices*

**List of Sample Output**

[request system snapshot media hard-disk on page 285](#)  
[request system snapshot media usb \(when usb device is missing on page 285](#)  
[request system snapshot media compact-flash on page 286](#)  
[request system snapshot media internal on page 286](#)  
[request system snapshot partition on page 286](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### [request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

### [request system snapshot media usb \(when usb device is missing](#)

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

```
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

#### request system snapshot media compact-flash

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

#### request system snapshot 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)

<b>Syntax</b>	request system software abort in-service-upgrade
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	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 <b>request system in-service-upgrade</b> 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.
<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>request system software in-service-upgrade (Maintenance)</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request system software abort in-service-upgrade on page 287</a>
<b>Output Fields</b>	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)

---

<b>Syntax</b>	<code>request system software add <i>package-name</i></code>
<b>Release Information</b>	Partition option introduced in the command in Release 10.1. of Junos OS.
<b>Description</b>	Installs the new software package on the device. For example: <b>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.</b>
<b>Options</b>	<ul style="list-style-type: none"><li>• <code>delay-restart</code> — Installs the software package but does not restart the software process</li><li>• <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors</li><li>• <code>no-copy</code> — Installs the software package but does not saves the copies of package files</li><li>• <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts</li><li>• <code>partition</code> — Formats and re-partitions the media before installation</li><li>• <code>reboot</code> — Reboots the device after installation is completed</li><li>• <code>unlink</code> — Removes the software package after successful installation</li><li>• <code>validate</code> — Checks the compatibility with current configuration before installation starts</li></ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li><li>• <i>Administration Guide for Security Devices</i></li></ul>

## request system reboot

<b>Syntax</b>	<code>request system reboot &lt;at time&gt; &lt;in minutes&gt;&lt;media&gt;&lt;message 'text'&gt;</code>
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Reboots the software.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <i>at time</i>— 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"> <li>• <i>now</i>— Reboots the device immediately. This is the default.</li> <li>• <i>+minutes</i>— Reboots the device in the number of minutes from now that you specify.</li> <li>• <i>yymmddhhmm</i>— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.</li> <li>• <i>hh:mm</i>— 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.</li> </ul> </li> <li>• <i>in minutes</i>— Specifies the number of minutes from now to reboot the device. This option is a synonym for the <i>at +minutes</i> option</li> <li>• <i>media type</i>— Specifies the boot device to boot the device from:             <ul style="list-style-type: none"> <li>• <i>disk/internal</i>— Reboots from the internal media. This is the default.</li> <li>• <i>usb</i>— Reboots from the USB storage device.</li> <li>• <i>compact flash</i>— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.</li> </ul> </li> <li>• <i>message text</i>— Provides a message to display to all system users before the device reboots.</li> </ul> <p>Example: <b>request system reboot at 5 in 50 media internal message stop</b></p>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system software rollback (Maintenance) on page 290</a></li> </ul>

## request system software rollback (Maintenance)

---

<b>Syntax</b>	request system software rollback <node <i>node-id</i> >   <all>   <local>   <primary> <reboot>
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Revert to the software that was loaded at the last successful <b>request system software add</b> command. Example: <b>request system software rollback</b> .
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>node <i>node-id</i></b>—(High-end SRX Series devices only) Roll back the software to the previous set of packages on a specific node.</li><li>• <b>all</b>— Roll back the software on all the nodes.</li><li>• <b>local</b>— Roll back the software on the local node.</li><li>• <b>primary</b>— Roll back the software on the primary node.</li><li>• <b>reboot</b>— Reboot the system after a roll back.</li></ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li><li>• <i>Administration Guide for Security Devices</i></li></ul>

## show chassis usb storage

<b>Syntax</b>	show chassis usb storage
<b>Release Information</b>	Command introduced in Junos OS Release 11.4 R2.
<b>Description</b>	Displays the current status of any USB mass storage device and whether the USB ports are enabled or disabled.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show chassis hardware detail on page 291</a> <a href="#">show chassis usb storage on page 291</a>

## 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
PIC
Power Supply

```

### show chassis usb storage

```

user@host> show chassis usb storage
USB Disabled

```

## show system autorecovery state

<b>Syntax</b>	show system autorecovery state
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Performs checks and shows status of all autorecovered items.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request system autorecovery state on page 273</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system autorecovery state on page 292</a>
<b>Output Fields</b>	Table 34 on page 292 lists the output fields for the <b>show system autorecovery state</b> command. Output fields are listed in the approximate order in which they appear.

Table 34: show system autorecovery state Output Fields

Field Name	Field Description
File	The name of the file on which autorecovery checks are performed.
Slice	The disk partition on which autorecovery checks are performed.
Recovery Information	Indicates whether autorecovery information for the file or slice has been saved.
Integrity Check	Displays the status of the file's integrity check (passed or failed).
Action / Status	Displays the status of the item, or the action required to be taken for that item.

## Sample Output

### show system autorecovery state

```
user@host> show system autorecovery state
```

```

Configuration:
File          Recovery Information  Integrity Check  Action / Status
rescue.conf.gz Saved                Passed           None
Licenses:
File          Recovery Information  Integrity Check  Action / Status
JUNOS282736.lic Saved                Passed           None
JUNOS282737.lic Not Saved           Not checked     Requires save
BSD Labels:
Slice         Recovery Information  Integrity Check  Action / Status
s1            Saved                Passed           None
s2            Saved                Passed           None

```

s3  
s4

Saved  
Saved

Passed  
Passed

None  
None

## show system auto-snapshot

<b>Syntax</b>	show system auto-snapshot
<b>Release Information</b>	Command introduced in Junos OS Release 12.1X45-D10.
<b>Description</b>	<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, <b>request system snapshot</b>.</p>
<b>Required Privilege Level</b>	View
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show system snapshot media on page 302</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system auto-snapshot on page 295</a>
<b>Output Fields</b>	<p><a href="#">Table 35 on page 294</a> lists the output fields for the <b>show system auto-snapshot</b> command. Output fields are listed in the approximate order in which they appear.</p>

**Table 35: show system auto-snapshot Output Fields**

Field Name	Field Description
<b>Auto-snapshot Configuration</b>	<p>Displays the configuration status of auto-snapshot.</p> <p>Status of the configuration:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—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.</li> <li>• <b>Disabled</b>—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, <b>request system snapshot</b>, to take a snapshot of one partition and copy it to the other.</li> </ul>
<b>Auto-snapshot State</b>	<p>Displays the current state of auto-snapshot.</p> <p>Status of the automatic snapshot procedure:</p> <ul style="list-style-type: none"> <li>• <b>Completed</b>—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared.</li> <li>• <b>Disabled</b>—The automatic snapshot procedure is inactive.</li> <li>• <b>In progress</b>—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size.</li> </ul>



## Sample Output

### show system auto-snapshot

```
user@host> show system auto-snapshot
```

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

## show system download

<b>Syntax</b>	<code>show system download &lt;download-id&gt;</code>
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Display a brief summary of all the download instances along with their current state and extent of progress. If a <b>download-id</b> is provided, the command displays a detailed report of the particular download instance.
<b>Options</b>	<ul style="list-style-type: none"> <li><b>download-id</b>—(Optional) The ID number of the download instance.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">request system download start on page 279</a></li> <li><i>Installation and Upgrade Guide for Security Devices</i></li> <li><i>Administration Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system download on page 296</a> <a href="#">show system download 1 on page 297</a>
<b>Output Fields</b>	Table 36 on page 296 lists the output fields for the <b>show system download</b> command. Output fields are listed in the approximate order in which they appear.

Table 36: 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)

<b>Syntax</b>	show system license <installed   keys   status   usage>
<b>Release Information</b>	Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.
<b>Description</b>	Display licenses and information about how licenses are used.
<b>Options</b>	<p><b>none</b>—Display all license information.</p> <p><b>installed</b>—(Optional) Display installed licenses only.</p> <p><b>keys</b>—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p><b>status</b>—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p><b>usage</b>—(Optional) Display the state of licensed features.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<p><a href="#">show system license on page 299</a></p> <p><a href="#">show system license installed on page 299</a></p> <p><a href="#">show system license keys on page 300</a></p> <p><a href="#">show system license usage on page 300</a></p> <p><a href="#">show system license status logical-system all on page 300</a></p>
<b>Output Fields</b>	Table 18 on page 121 lists the output fields for the <b>show system license</b> command. Output fields are listed in the approximate order in which they appear.

**Table 37: show system license Output Fields**

Field Name	Field Description
<b>Feature name</b>	Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.
<b>Licenses used</b>	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 37: show system license Output Fields (*continued*)

Field Name	Field Description
Licenses installed	Information about the installed license key: <ul style="list-style-type: none"> <li>• <b>License identifier</b>—Identifier associated with a license key.</li> <li>• <b>License version</b>—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.</li> <li>• <b>Valid for device</b>—Device that can use a license key.</li> <li>• <b>Features</b>—Feature associated with a license.</li> </ul>
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

<b>Syntax</b>	show system login logout
<b>Release Information</b>	Command introduced in Release 11.2 of Junos OS.
<b>Description</b>	Display the user names locked after unsuccessful login attempts.
<b>Required Privilege Level</b>	view and system
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show system login logout on page 301</a>
<b>Output Fields</b>	Table 38 on page 301 lists the output fields for the <b>show system login logout</b> 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 <b>detail</b> keyword is used.

Table 38: show system login logout

Field Name	Field Description	Level of Output
User	Username	All levels
Lockout start	Date and time the username was locked	All levels
Lockout end	Date and time the username was unlocked	All levels

## Sample Output

### show system login logout

```
user@host>show system login logout
```

```

User           Lockout start      Lockout end
root          2011-05-11 09:11:15 UTC 2011-05-11 09:13:15 UTC

```

## show system snapshot media

---

<b>Syntax</b>	show system snapshot media <i>media-type</i>
<b>Release Information</b>	Command introduced in Release 10.2 of Junos OS.
<b>Description</b>	Display the snapshot information for both root partitions on SRX Series devices
<b>Options</b>	<ul style="list-style-type: none"><li>• internal— Show snapshot information from internal media.</li><li>• usb— Show snapshot information from device connected to USB port.</li><li>• external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.</li></ul>
<b>Required Privilege Level</b>	View
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>

### 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 39 on page 303](#) describes the output fields for the **show system storage** command. Output fields are listed in the approximate order in which they appear.

**Table 39: show system storage Output Fields**

Field Name	Field Description
<b>Filesystem</b>	Name of the file system.
<b>Size</b>	Size of the file system.
<b>Used</b>	Amount of space used in the file system.

Table 39: show system storage Output Fields (*continued*)

Field Name	Field Description
<b>Avail</b>	Amount of space available in the file system.
<b>Capacity</b>	Percentage of the file system space that is being used.
<b>Mounted on</b>	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)

<b>Syntax</b>	show system storage partitions
<b>Release Information</b>	Command introduced in Release 10.2 of Junos OS.
<b>Description</b>	Displays the partitioning scheme details on SRX Series devices.
<b>Required Privilege Level</b>	View
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>

## 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

---

<b>Syntax</b>	<code>show version</code> <code>&lt;brief   detail&gt;</code> <code>&lt;node <i>node-id</i>   local   primary&gt;</code>
<b>Release Information</b>	Command introduced in Junos OS Release 10.4.
<b>Description</b>	Display the hostname and version information about the software running on the device.
<b>Options</b>	<b>none</b> —Display standard information about the hostname and version of the software running on the device.  <b>brief</b> —Display brief output.  <b>detail</b> —Display detailed output.  <b>node <i>node-id</i></b> —Display the software version on a specific node. <b>Range:</b> 0 through 1  <b>local</b> —Display the software version on the local node.  <b>primary</b> —Display the software version on the primary node.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Determining the Junos OS Version on page 170</a></li></ul>
<b>List of Sample Output</b>	<a href="#">show version on page 306</a>

## 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 309](#)
- [Configuration on page 357](#)
- [Administration on page 493](#)
- [Troubleshooting on page 569](#)



## CHAPTER 8

# Overview

- [CLI Overview on page 309](#)
- [CLI Online Help on page 315](#)
- [CLI Operational Mode on page 319](#)
- [CLI Configuration Mode on page 334](#)
- [CLI Advanced Features on page 347](#)
- [CLI Commit Operations on page 350](#)
- [Configuration Groups on page 353](#)
- [Configuration Management on page 354](#)

## CLI Overview

---

- [Introducing the Junos OS Command-Line Interface on page 309](#)
- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 311](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 314](#)
- [Commands and Configuration Statements for Junos-FIPS on page 314](#)

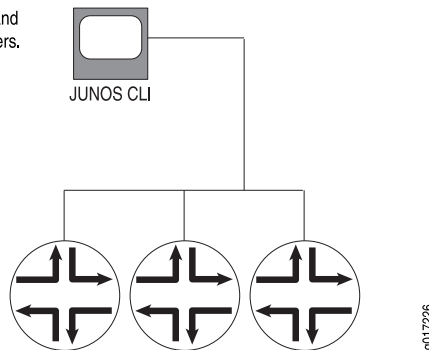
## Introducing the Junos OS Command-Line Interface

The 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 8 on page 310](#)). The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press Enter.

**Figure 8: Monitoring and Configuring Routers**

Use the JUNOS CLI to monitor and configure Juniper Networks routers.



### Key Features of the CLI

The Junos OS CLI commands and statements follow a hierarchal organization and have a regular syntax. The Junos OS CLI provides the following features to simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software on which they are operating. For example, all **show** commands display software information and statistics, and all **clear** commands erase various types of system information.
- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command. This means that if you already are familiar with the Junos OS or with other routing software, you can use many of the CLI commands without referring to the documentation.
- Command completion—Command completion for command names (keywords) and for command options is available at each level of the hierarchy. To complete a command or option that you have partially typed, press the Tab key or the Spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command, and the possible completions are displayed. Completion also applies to other strings, such as filenames, interface names, usernames, and configuration statements.

If you have typed the mandatory arguments for executing a command in the operational or configuration mode the CLI displays **<[Enter]>** as one of the choices when you type a question mark (?). This indicates that you have entered the mandatory arguments and can execute the command at that level without specifying any further options. Likewise, the CLI also displays **<[Enter]>** when you have reached a specific hierarchy level in the configuration mode and do not have to enter any more mandatory arguments or statements.

- Industry-standard technology—With FreeBSD UNIX as the kernel, a variety of UNIX utilities are available on the Junos OS CLI. For example, you can:
  - Use regular expression matching to locate and replace values and identifiers in a configuration, filter command output, or examine log file entries.



- Use Emacs-based key sequences to move around on a command line and scroll through the recently executed commands and command output.
- Store and archive Junos OS device files on a UNIX-based file system.
  - Use standard UNIX conventions to specify filenames and paths.
- Exit from the CLI environment and create a UNIX C shell or Bourne shell to navigate the file system, manage router processes, and so on.

**Related Documentation**

- [Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies on page 311](#)
- [Getting Started with the Junos OS Command-Line Interface on page 368](#)
- [Other Tools to Configure and Monitor Devices Running Junos OS on page 314](#)
- [Commands and Configuration Statements for Junos-FIPS on page 314](#)

## 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 311](#)
- [CLI Command Hierarchy on page 312](#)
- [Configuration Statement Hierarchy on page 312](#)
- [Moving Among Hierarchy Levels on page 313](#)

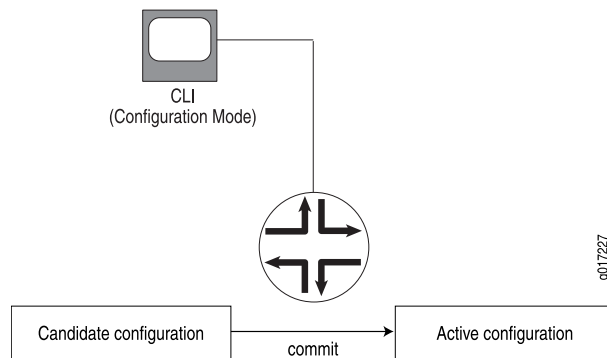
### Junos OS CLI Command Modes

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 9 on page 312](#)). Candidate configurations enable you to alter your configuration without causing potential damage to your current network operations.

Figure 9: 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.

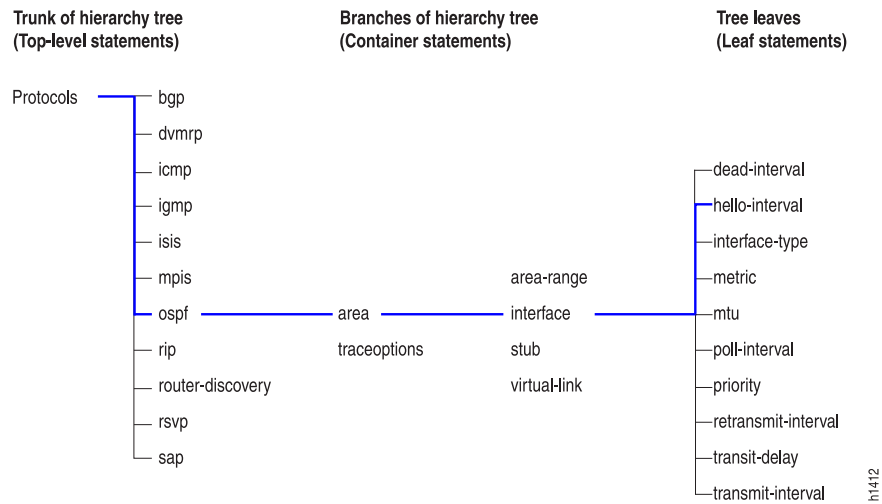
To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of the routes in the routing table, use the command **show route brief**.

### 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 10 on page 313 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 10: Configuration Statement Hierarchy Example



### Moving Among Hierarchy Levels

You can use the CLI commands in [Table 40 on page 313](#) to navigate the levels of the configuration statement hierarchy.

Table 40: CLI Configuration Mode Navigation Commands

Command	Description
<b>edit</b> <i>hierarchy-level</i>	Moves to an existing configuration statement hierarchy or creates a hierarchy and moves to that level.
<b>exit</b>	Moves up the hierarchy to the previous level where you were working. This command is, in effect, the opposite of the <b>edit</b> command. Alternatively, you can use the <b>quit</b> command. The <b>exit</b> and <b>quit</b> commands are interchangeable.
<b>up</b>	Moves up the hierarchy one level at a time.
<b>top</b>	Moves directly to the top level of the hierarchy.

#### Related Documentation

- [Introducing the Junos OS Command-Line Interface on page 309](#)
- [Getting Started with the Junos OS Command-Line Interface on page 368](#)

## 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 *Junos OS Configuration and Operations Automation Library*.
- 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

- [Introducing the Junos OS Command-Line Interface on page 309](#)
- [Getting Started with the Junos OS Command-Line Interface on page 368](#)
- [Commands and Configuration Statements for Junos-FIPS on page 314](#)

## Commands and Configuration Statements for Junos-FIPS

Junos-FIPS enables you to configure a network of Juniper Networks routers in a Federal Information Processing Standards (FIPS) 140-2 environment.

The Junos-FIPS software environment requires the installation of FIPS software by a crypto officer. In Junos-FIPS, some Junos OS commands and statements have restrictions and some additional configuration statements are available. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

### Related Documentation

- [Junos Secure Configuration Guide for Common Criteria and Junos-FIPS](#)

## CLI Online Help

- [Getting Online Help from the Junos OS Command-Line Interface on page 315](#)
- [Junos OS CLI Online Help Features on page 317](#)

### 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 315](#)
- [Getting Help About a String in a Statement or Command on page 316](#)
- [Getting Help About Configuration Statements on page 316](#)
- [Getting Help About System Log Messages on page 317](#)

#### 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 317](#)
- [Getting Started with the Junos OS Command-Line Interface on page 368](#)

## 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 317](#)
- [Using CLI Command Completion on page 318](#)
- [Using Command Completion in Configuration Mode on page 318](#)
- [Displaying Tips About CLI Commands on page 318](#)

### 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 368](#)
- [Examples: Using the Junos OS CLI Command Completion on page 454](#)

## CLI Operational Mode

- [Overview of Junos OS CLI Operational Mode Commands on page 319](#)
- [Junos OS Operational Mode Commands That Combine Other Commands on page 322](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 322](#)
- [Controlling the Scope of an Operational Mode Command on page 323](#)
- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)
- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 328](#)

## 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 319](#)
- [Commonly Used Operational Mode Commands on page 320](#)

### 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 311.
- 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 334.
- A command—**quit**—to exit the CLI. For information about this command, see [CLI Explorer](#).

### Commonly Used Operational Mode Commands

Table 41 on page 320 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 41: 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>

Table 41: Commonly Used Operational Mode Commands (*continued*)

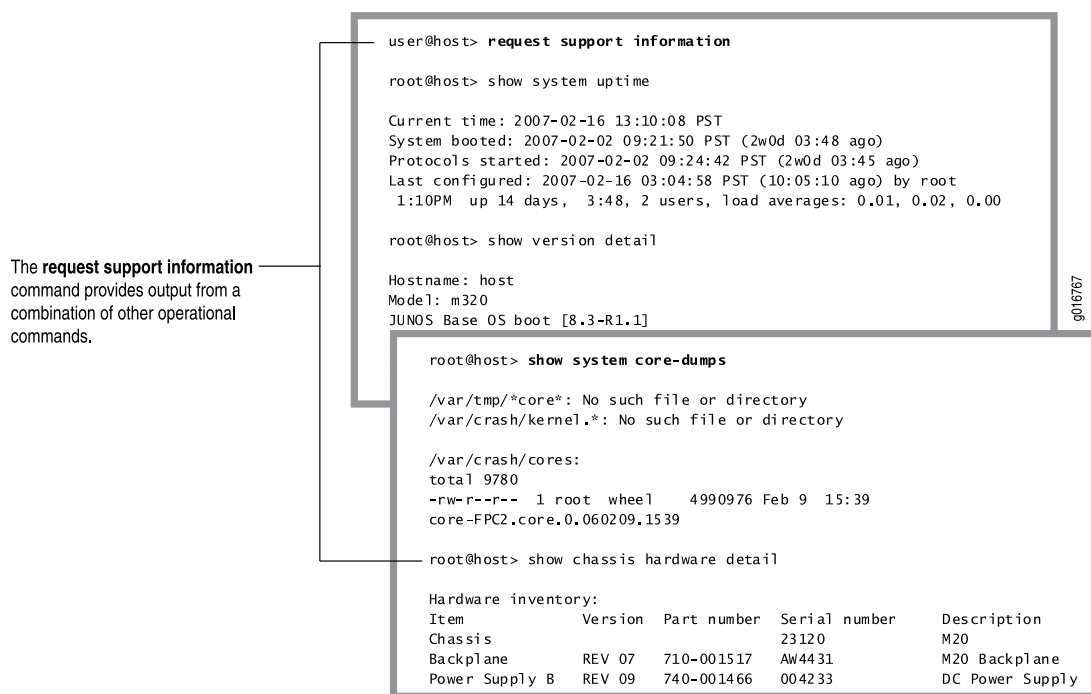
Items to Check	Description	Command
Log files	Contents of the log files	<b>monitor</b>
	Log files and their contents and recent user logins	<b>show log</b>
Remote systems	Host reachability and network connectivity	<b>ping</b>
	Route to a network system	<b>tracert</b>
Configuration	Current system configuration	<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>
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 322](#)
  - [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 322](#)

## 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 11 on page 322](#).

**Figure 11: Commands That Combine Other Commands**



- Related Documentation**
- [Overview of Junos OS CLI Operational Mode Commands on page 319](#)
  - [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 322](#)

## 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 12 on page 323](#).)

Figure 12: 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 319](#)
- [Controlling the Scope of an Operational Mode Command on page 323](#)

## 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, mpIs:
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)---

- 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 493](#)



- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 508](#)

## 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 328](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)

## 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 42: 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:

```
1 2
2 2
3 2 1
4
```

a pipe filter of **| match 2** displays the following output:

```
1 2
2 2
3 2 1
```

and a pipe filter of **| except 1** displays the following output:

```
2 2
4
```

#### Related Documentation

- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)
- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 328](#)

## 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 329](#)
- [Counting the Number of Lines of Output on page 330](#)
- [Displaying Output in XML Tag Format on page 330](#)
- [Displaying the RPC tags for a Command on page 331](#)
- [Ignoring Output That Does Not Match a Regular Expression on page 331](#)
- [Displaying Output from the First Match of a Regular Expression on page 331](#)

- [Retaining Output After the Last Screen on page 332](#)
- [Displaying Output Beginning with the Last Entries on page 332](#)
- [Displaying Output That Matches a Regular Expression on page 332](#)
- [Preventing Output from Being Paginated on page 333](#)
- [Sending Command Output to Other Users on page 333](#)
- [Resolving IP Addresses on page 333](#)
- [Saving Output to a File on page 334](#)
- [Trimming Output by Specifying the Starting Column on page 334](#)

### 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 327](#).

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 327](#).

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 327.

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

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 327](#)
- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)

## [CLI Configuration Mode](#)

---

- [Understanding Junos OS CLI Configuration Mode on page 334](#)
- [Modifying the Junos OS Configuration on page 341](#)
- [Commit Operation When Multiple Users Configure the Software on page 341](#)
- [Forms of the configure Command on page 342](#)
- [Additional Details About Specifying Junos Statements and Identifiers on page 344](#)

### [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 311, 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 43 on page 336 summarizes each CLI configuration mode command. The commands are organized alphabetically.

**Table 43: Summary of Configuration Mode Commands**

Command	Description
<b>activate</b>	Remove the <b>inactive:</b> 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 <b>commit</b> command.
<b>annotate</b>	Add comments to a configuration. You can add comments only at the current hierarchy level.
<b>commit</b>	Commit the set of changes to the database and cause the changes to take operational effect.
<b>copy</b>	Make a copy of an existing statement in the configuration.
<b>deactivate</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>delete</b>	Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.
<b>edit</b>	Move inside the specified statement hierarchy. If the statement does not exist, it is created.
<b>exit</b>	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The <b>quit</b> and <b>exit</b> commands are synonyms.
<b>extension</b>	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.
<b>help</b>	Display help about available configuration statements.
<b>insert</b>	Insert an identifier into an existing hierarchy.
<b>load</b>	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 43: Summary of Configuration Mode Commands (*continued*)

Command	Description
<b>quit</b>	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The <b>quit</b> and <b>exit</b> commands are synonyms.
<b>rename</b>	Rename an existing configuration statement or identifier.
<b>replace</b>	Replace identifiers or values in a configuration.
<b>rollback</b>	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 <b>commit configuration</b> command.
<b>run</b>	Run a top-level CLI command without exiting from configuration mode.
<b>save</b>	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.
<b>set</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>show</b>	Display the current configuration.
<b>status</b>	Display the users currently editing the configuration.
<b>top</b>	Return to the top level of configuration command mode, which is indicated by the <b>[edit]</b> banner.
<b>up</b>	Move up one level in the statement hierarchy.
<b>update</b>	Update a private database.
<b>wildcard</b>	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 44 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 44: Configuration Mode Top-Level Statements**

Statement	Description
<b>access</b>	Configure the Challenge Handshake Authentication Protocol (CHAP).
<b>accounting-options</b>	Configure accounting statistics data collection for interfaces and firewall filters. .
<b>chassis</b>	Configure properties of the router chassis, including conditions that activate alarms and SONET/SDH framing and concatenation properties. .
<b>class-of-service</b>	Configure class-of-service parameters. For information about the statements in this hierarchy, see the <i>Junos OS CoS Library for Security Devices</i> .
<b>firewall</b>	Define filters that select packets based on their contents. .
<b>forwarding-options</b>	Define forwarding options, including traffic sampling options. .
<b>groups</b>	Configure configuration groups. .
<b>interfaces</b>	Configure interface information, such as encapsulation, interfaces, virtual channel identifiers (VCIs), and data-link connection identifiers (DLCIs). For information about the statements in this hierarchy, see the <i>Junos OS Interfaces Library for Security Devices</i> .
<b>policy-options</b>	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes. .
<b>protocols</b>	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> .
<b>routing-instances</b>	Configure multiple routing instances. For information about the statements in this hierarchy, see the <i>Junos OS Routing Protocols Library for Security Devices</i> .
<b>routing-options</b>	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> .
<b>security</b>	Configure IP Security (IPsec) services. .

Table 44: Configuration Mode Top-Level Statements (*continued*)

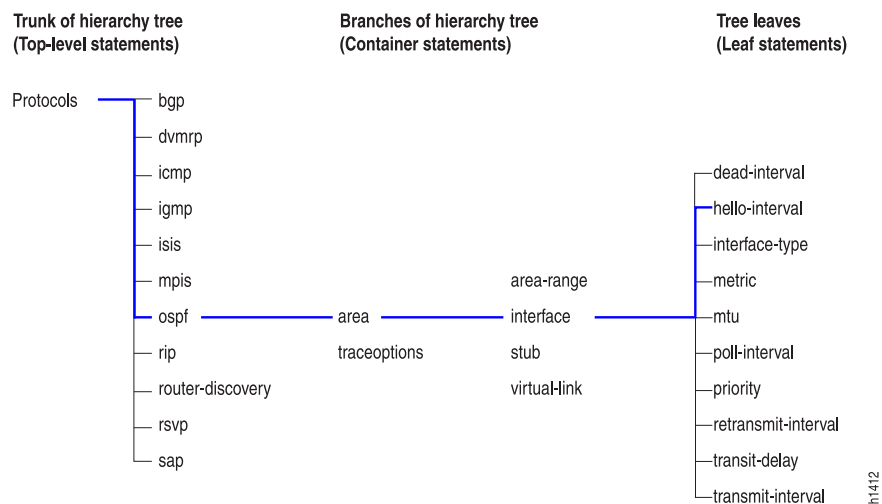
Statement	Description
<b>snmp</b>	Configure SNMP community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the <i>SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices</i> .
<b>system</b>	Configure systemwide properties, 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 358](#)

## 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 360](#)
- [Adding Junos Configuration Statements and Identifiers on page 380](#)
- [Using the configure exclusive Command on page 367](#)
- [Updating the configure private Configuration on page 368](#)
- [Issuing Relative Junos Configuration Mode Commands on page 385](#)

## 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 406](#)
- [Forms of the configure Command on page 342](#)
- [Displaying Users Currently Editing the Configuration on page 364](#)

## 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 45 on page 343](#).



Table 45: Forms of the configure Command

Command	Edit Access	Commit Access
<b>configure</b>	<ul style="list-style-type: none"> <li>No one can lock the configuration. All users can make configuration changes.</li> </ul> <p>When you enter configuration mode, the CLI displays the following information:</p> <ul style="list-style-type: none"> <li>A list of other users editing the configuration.</li> <li>Hierarchy levels the users are viewing or editing.</li> <li>Whether the configuration has been changed, but not committed.</li> <li>When multiple users enter conflicting configurations, the most recent change to be entered takes precedence.</li> </ul>	<ul style="list-style-type: none"> <li>No one can lock the configuration. All users can commit all changes to the configuration.</li> <li>If you and another user make changes and the other user commits changes, your changes are committed as well.</li> </ul>
<b>configure exclusive</b>	<ul style="list-style-type: none"> <li>One user locks the configuration and makes changes without interference from other users.</li> <li>Other users can enter and exit configuration mode, but they cannot commit the configuration.</li> <li>If you enter configuration mode while another user has locked the configuration (with the <b>configure exclusive</b> command), the CLI displays the user and the hierarchy level the user is viewing or editing.</li> <li>If you enter configuration mode while another user has locked the configuration, you can forcibly log out that user with the <b>request system logout</b> operational mode command. For details, see <a href="#">CLI Explorer</a>.</li> </ul>	
<b>configure private</b>	<ul style="list-style-type: none"> <li>Multiple users can edit the configuration at the same time.</li> <li>Each user has a private candidate configuration to edit independently of other users.</li> <li>When multiple users enter conflicting configurations, the first commit operation takes precedence over subsequent commit operations.</li> </ul>	<ul style="list-style-type: none"> <li>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.</li> <li>If the configuration has been modified by another user, you can merge the modifications into your private candidate configuration and attempt to commit again.</li> </ul>

**Related Documentation**

- [Committing a Junos OS Configuration on page 406](#)
- [Example: Using the configure Command on page 455](#)
- [Displaying Users Currently Editing the Configuration on page 364](#)
- [Using the configure exclusive Command on page 367](#)
- [Updating the configure private Configuration on page 368](#)
- [Displaying set Commands from the Junos OS Configuration on page 361](#)

## 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 344](#)
- [Performing CLI Type-Checking on page 346](#)

### 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 46 on page 346](#) lists the data types the CLI checks.

**Table 46: CLI Configuration Input Types**

Data Type	Format	Examples
Physical interface name (used in the <b>[edit interfaces]</b> hierarchy)	<i>type-fpc/pic/port</i>	Correct: so-0/0/1  Incorrect: so-0
Full interface name	<i>type-fpc/pic/port&lt;:channel&gt;.logical</i>	Correct: so-0/0/1.0  Incorrect: so-0/0/1
Full or abbreviated interface name (used in places other than the <b>[edit interfaces]</b> hierarchy)	<i>type-&lt;fpc&lt;/pic/port&gt;&gt;&lt;&lt;:channel&gt;.logical&gt;</i>	Correct: so, so-1, so-1/2/3:4.5
IP address	<i>0xhex-bytesoctet&lt;.octet&lt;.octet&lt;.octet&gt;&gt;&gt;</i>	Correct: 1.2.3.4, 0x01020304, 128.8.1, 128.8  Sample translations:  1.2.3 becomes 1.2.3.0 0x01020304 becomes 1.2.3.4 0x010203 becomes 0.1.2.3
IP address (destination prefix) and prefix length	<i>0xhex-bytes&lt;/length&gt;octet&lt;octet&lt;.octet&lt;.octet&gt;&gt;&gt;&lt;/length&gt;</i>	Correct: 10/8, 128.8/16, 1.2.3.4/32, 1.2.3.4  Sample translations:  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
International Organization for Standardization (ISO) address	<i>hex-nibble&lt;hex-nibble ...&gt;</i>	Correct: 47.1234.2345.3456.00, 47.123423453456.00, 47.12.34.23.45.34.56.00  Sample translations:  47123456 becomes 47.1234.56 47.12.34.56 becomes 47.1234.56 4712.3456 becomes 47.1234.56

Table 46: CLI Configuration Input Types *(continued)*

Data Type	Format	Examples
OSPF area identifier (ID)	<i>0xhex-bytesoctet&lt;.octet&lt;.octet.&lt; octet &gt;&gt;&gt; decimal-number</i>	<p><b>Correct:</b> 54, 0.0.0.54, 0x01020304, 1.2.3.4</p> <p><b>Sample translations:</b></p> <p>54 becomes 0.0.0.54</p> <p>257 becomes 0.0.1.1</p> <p>128.8 becomes 128.8.0.0</p> <p>0x010203 becomes 0.1.2.3</p>

**Related Documentation**

- [Entering and Exiting the Junos OS CLI Configuration Mode on page 358](#)

## CLI Advanced Features

- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 347](#)
- [Using Wildcard Characters in Interface Names on page 349](#)
- [Using Global Replace in a Junos Configuration on page 349](#)

### 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 47 on page 347](#) lists some of the CLI keyboard sequences. They are the same as those used in Emacs.

Table 47: 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

Table 47: CLI Keyboard Sequences (*continued*)

Category	Action	Keyboard Sequence
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
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> <i>sequence</i> or Alt+ <i>number</i> <i>sequence</i>

**Related Documentation**

- [Using Wildcard Characters in Interface Names on page 349](#)

- [Using Global Replace in a Junos Configuration on page 349](#)

## 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 48 on page 349](#) lists the available wildcard characters. You must enclose all wildcard characters except the asterisk (\*) in quotation marks (" ").

**Table 48: Wildcard Characters for Specifying Interface Names**

Wildcard Character	Description
<b>* (asterisk)</b>	Match any string of characters in that position in the interface name. For example, <b>so*</b> matches all SONET/SDH interfaces.
<b>"[character&lt;character...&gt;]"</b>	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.
<b>"[!character&lt;character...&gt;]"</b>	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.
<b>"[character1-character2]"</b>	Match a range of characters. For example, <b>so-"[0-3]"*</b> matches all SONET/SDH interfaces in slots 0, 1, 2, and 3.
<b>"[!character1-character2]"</b>	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 347](#)
- [Using Global Replace in a Junos Configuration on page 349](#)

## 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 516](#)
- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 456](#)
- [Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name on page 457](#)
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 458](#)
- [Using Wildcard Characters in Interface Names on page 349](#)
- [Using Keyboard Sequences to Move Around and Edit the Junos OS CLI on page 347](#)

---

## CLI Commit Operations

- [Junos OS Commit Model for Router or Switch Configuration on page 350](#)
- [Commit Operation When Multiple Users Configure the Software on page 351](#)
- [Junos OS Batch Commits Overview on page 352](#)

### 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*

## 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 406](#)
- [Forms of the configure Command on page 342](#)
- [Displaying Users Currently Editing the Configuration on page 364](#)

## 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**.

## Configuration Groups

---

- [Understanding the Junos Configuration Groups on page 353](#)

### 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 353](#)
- [Inheritance Model on page 354](#)
- [Configuring Configuration Groups on page 354](#)

#### 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 428](#)

## Configuration Management

---

- [Understanding How the Junos Configuration Is Stored on page 354](#)

### 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 569](#)
- [Returning to a Previously Committed Junos OS Configuration on page 569](#)
- [Loading a Configuration from a File on page 421](#)



## CHAPTER 9

# Configuration

- [Getting Started with Junos OS Configuration on page 357](#)
- [Updating the Junos OS Configuration on page 380](#)
- [Committing a Junos OS Configuration on page 398](#)
- [Loading a Junos OS Configuration on page 421](#)
- [Synchronizing the Junos OS Configuration on page 426](#)
- [Creating and Applying Junos OS Configuration Groups on page 427](#)
- [CLI Online Help on page 452](#)
- [CLI Configuration Mode on page 455](#)
- [Controlling the CLI Environment on page 456](#)
- [CLI Advanced Features on page 456](#)
- [Configuration Statements on page 460](#)

### Getting Started with Junos OS Configuration

- [Entering and Exiting the Junos OS CLI Configuration Mode on page 358](#)
- [Displaying the Current Junos OS Configuration on page 360](#)
- [Example: Displaying the Current Junos OS Configuration on page 360](#)
- [Displaying set Commands from the Junos OS Configuration on page 361](#)
- [Displaying Users Currently Editing the Configuration on page 364](#)
- [Displaying Additional Information About the Configuration on page 364](#)
- [Using the configure exclusive Command on page 367](#)
- [Updating the configure private Configuration on page 368](#)
- [Getting Started with the Junos OS Command-Line Interface on page 368](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 370](#)
- [Configuring a User Account on a Device Running Junos OS on page 372](#)
- [Example: Configuring a Routing Protocol on page 374](#)

## 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 *Access Privilege Administration Guide*.

- 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 334](#)
- [Modifying the Junos OS Configuration on page 341](#)
- [Commit Operation When Multiple Users Configure the Software on page 341](#)
- [Displaying the Current Junos OS Configuration on page 360](#)
- [Displaying set Commands from the Junos OS Configuration on page 361](#)
- [Issuing Relative Junos Configuration Mode Commands on page 385](#)
- [Using the configure exclusive Command on page 367](#)
- [Updating the configure private Configuration on page 368](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 370](#)

## 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 360](#)
- [Displaying set Commands from the Junos OS Configuration on page 361](#)

## 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 360](#)

## 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 362](#)
- [Example: Displaying Required set Commands at the Current Hierarchy Level on page 362](#)
- [Example: Displaying set Commands with the match Option on page 363](#)

#### 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 360](#)

## 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 410](#).

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 342](#)
- [Using the configure exclusive Command on page 367](#)

## 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 361](#)

## 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 380](#)
- [Forms of the configure Command on page 342](#)

## Updating the configure private Configuration

When you are in configure private mode, you must work with a copy of the most recently committed shared configuration. If the global configuration changes, you can issue the **update** command to update your private candidate configuration. When you do this, your private candidate configuration contains a copy of the most recently committed configuration with your private changes merged in. For example:

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



**NOTE:** Merge conflicts can occur when you issue the **update** command.

You can also issue the **rollback** command to discard your private candidate configuration changes and obtain the most recently committed configuration:

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

**Related  
Documentation**

- [Forms of the configure Command on page 342](#)

## 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
tracert	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 315](#)
- [Switching Between Junos OS CLI Operational and Configuration Modes on page 370](#)
- [Checking the Status of a Device Running Junos OS on page 495](#)
- [Configuring a User Account on a Device Running Junos OS on page 372](#)
- [Example: Configuring a Routing Protocol on page 374](#)
- [Examples: Using the Junos OS CLI Command Completion on page 454](#)

## 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 311](#)
  - [Getting Online Help from the Junos OS Command-Line Interface on page 315](#)
  - [Configuring a User Account on a Device Running Junos OS on page 372](#)

## 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).

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 feature guides.

#### Related Documentation

- [Getting Started with the Junos OS Command-Line Interface on page 368](#)
- [Getting Online Help from the Junos OS Command-Line Interface on page 315](#)
- [Displaying the Junos OS CLI Command and Word History on page 455](#)
- [Example: Configuring a Routing Protocol on page 374](#)

## 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 375](#)
- [Longer Configuration on page 375](#)
- [Making Changes to a Routing Protocol Configuration on page 377](#)

### 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 368](#)
- [Displaying the Junos OS CLI Command and Word History on page 455](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 493](#)

---

## Updating the Junos OS Configuration

- [Adding Junos Configuration Statements and Identifiers on page 380](#)
- [Deleting a Statement from a Junos Configuration on page 382](#)
- [Example: Deleting a Statement from the Junos Configuration on page 383](#)
- [Copying a Junos Statement in the Configuration on page 384](#)
- [Example: Copying a Statement in the Junos Configuration on page 384](#)
- [Issuing Relative Junos Configuration Mode Commands on page 385](#)
- [Renaming an Identifier in a Junos Configuration on page 385](#)
- [Example: Renaming an Identifier in a Junos Configuration on page 386](#)
- [Inserting a New Identifier in a Junos Configuration on page 386](#)
- [Example: Inserting a New Identifier in a Junos Configuration on page 386](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 388](#)
- [Examples: Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 389](#)
- [Adding Comments in a Junos Configuration on page 390](#)
- [Example: Including Comments in a Junos Configuration on page 391](#)
- [Using Regular Expressions to Delete Related Items from a Junos Configuration on page 393](#)
- [Example: Using the Wildcard Command with the Range Option on page 394](#)

### 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 341](#)
- [Deleting a Statement from a Junos Configuration on page 382](#)
- [Copying a Junos Statement in the Configuration on page 384](#)
- [Renaming an Identifier in a Junos Configuration on page 385](#)
- [Using the configure exclusive Command on page 367](#)

- [Additional Details About Specifying Junos Statements and Identifiers on page 344](#)
- [Displaying the Current Junos OS Configuration on page 360](#)

## 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 383](#)
  - [Adding Junos Configuration Statements and Identifiers on page 380](#)
  - [Copying a Junos Statement in the Configuration on page 384](#)

## 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 458](#)
- [Deleting a Statement from a Junos Configuration on page 382](#)

## 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 384](#)
- [Adding Junos Configuration Statements and Identifiers on page 380](#)

## 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 384](#)

## 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 360](#)

## 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 380](#)
  - [Example: Renaming an Identifier in a Junos Configuration on page 386](#)
  - [Inserting a New Identifier in a Junos Configuration on page 386](#)

### 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 385](#)

### 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 385](#)
  - [Example: Renaming an Identifier in a Junos Configuration on page 386](#)
  - [Example: Inserting a New Identifier in a Junos Configuration on page 386](#)
  - [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 388](#)

### 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 term4 to term term6
[edit]
user@host# set policy-options policy-statement statics term term4 from protocol local
[edit]
user@host# set policy-options policy-statement statics term term4 then reject
[edit]
user@host# set policy-options policy-statement statics term term5 from protocol
aggregate
[edit]
user@host# set policy-options policy-statement statics term term5 then reject
[edit]
user@host# insert policy-options policy-statement statics term term4 after term term3
[edit]
user@host# insert policy-options policy-statement statics term term5 after term term4
[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 386](#)
- [Adding Junos Configuration Statements and Identifiers on page 380](#)

## 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 389](#)
- [Adding Junos Configuration Statements and Identifiers on page 380](#)

## 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 388](#)

## 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 380](#)
  - [Example: Including Comments in a Junos Configuration on page 391](#)

## 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 390](#)

## 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 433](#)

**Example: Using the Wildcard Command with the Range Option**

- [Requirements on page 394](#)
- [Overview on page 394](#)
- [Configuration on page 395](#)
- [Verification on page 397](#)

---

**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 395](#)
- [Specifying Multiple Ranges in the Syntax on page 396](#)
- [Specifying a Range and Unique Numbers In the Syntax on page 396](#)
- [Excluding Some Values from a Range on page 396](#)
- [Specifying a Range with a Step Number on page 397](#)

### *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 397](#)

### **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 395](#).

**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 349](#)

---

## Committing a Junos OS Configuration

- [Verifying a Junos Configuration on page 399](#)
- [Example: Protecting the Junos OS Configuration from Modification or Deletion on page 399](#)
- [Committing a Junos OS Configuration on page 406](#)
- [Committing a Junos Configuration and Exiting Configuration Mode on page 408](#)
- [Activating a Junos Configuration but Requiring Confirmation on page 409](#)
- [Scheduling a Junos Commit Operation on page 410](#)
- [Monitoring the Junos Commit Process on page 411](#)
- [Adding a Comment to Describe the Committed Configuration on page 412](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 413](#)
- [Example: Configuring Junos OS Batch Commits on page 414](#)



## 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 380](#)
  - [Committing a Junos OS Configuration on page 406](#)

## 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 399](#)
- [Overview on page 399](#)
- [Protecting a Parent-Level Hierarchy on page 400](#)
- [Protecting a Child Hierarchy on page 400](#)
- [Protecting a Configuration Statement Within a Hierarchy on page 401](#)
- [Protecting a List of Identifiers for a Configuration Statement on page 401](#)
- [Protecting an Individual Member from a Homogenous List on page 402](#)
- [Unprotecting a Configuration on page 402](#)
- [Verification on page 402](#)

### Requirements

This example uses the following hardware and software components:

- A J Series, 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];
}
```

- 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.

## Committing a Junos OS Configuration

To save Junos OS configuration changes to the configuration database and to activate the configuration on the router, use the **commit** configuration mode command. You can issue the **commit** command from any hierarchy level:

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

When you enter the **commit** command, the configuration is first checked for syntax errors (**commit check**). Then, if the syntax is correct, the configuration is activated and becomes the current, operational router configuration.

You can issue the **commit** command from any hierarchy level.

A configuration commit can fail for any of the following reasons:

- The configuration includes incorrect syntax, which causes the commit check to fail.
- The candidate configuration that you are trying to commit is larger than 700 MB.
- The configuration is locked by a user who entered the **configure exclusive** command.

If the configuration contains syntax errors, a message indicates the location of the error, and the configuration is not activated. The error message has the following format:

```
[edit edit-path]
'offending-statement;'
error-message
```

For example:

```
[edit firewall filter login-allowed term allowed from]
```



```
'icmp-type [ echo-request echo-reply ];'
keyword 'echo-reply' unrecognized
```

You must correct the error before recommitting the configuration. To return quickly to the hierarchy level where the error is located, copy the path from the first line of the error and paste it at the configuration mode prompt at the **[edit]** hierarchy level.

The uncommitted, candidate configuration file is `/var/run/db/juniper.db`. It is limited to 700 MB. If the commit fails with a message **configuration database size limit exceeded**, view the file size from configuration mode by entering the command `run file list /var/run/db detail`. You can simplify the configuration and reduce the file size by creating configuration groups with wildcards or defining less specific match policies in your firewall filters.



**NOTE:** CLI commit-time warnings displayed for configuration changes at the **[edit interfaces]** hierarchy level are removed and are logged as system log messages.

This is also applicable to VRRP configuration at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* family (*inet* | *inet6*) address *address*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (*inet* | *inet6*) address *address*]**

When you commit a configuration, you commit the entire configuration in its current form. If more than one user is modifying the configuration, committing it saves and activates the changes of all the users.

**NOTE:**

- If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

load merge  
load replace  
load override  
load update

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

- We do not recommend performing a commit operation on the backup Routing Engine when graceful Routing Engine switchover is enabled on the router.



**NOTE:** If you configure the same IP address for a management interface or internal interface such as fxp0 and an external physical interface such as ge-0/0/1, when graceful Routing Engine switchover (GRES) is enabled, the CLI displays an appropriate commit error message that identical addresses have been found on the private and public interfaces. In such cases, you must assign unique IP addresses for the two interfaces that have duplicate addresses.

The management Ethernet interface used for the TX Matrix Plus router, T1600 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 408](#)
- [Activating a Junos Configuration but Requiring Confirmation on page 409](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 413](#)
- [Forms of the configure Command on page 342](#)

## 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 409](#)

## 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:

```

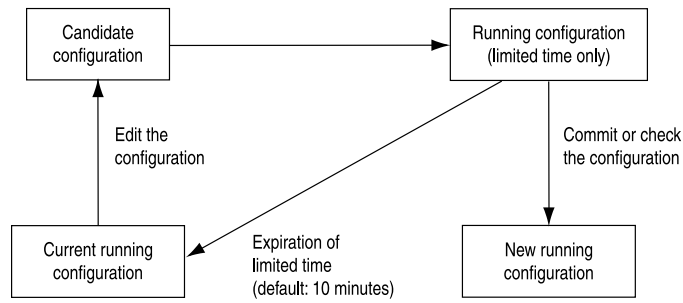
user@host> show system commit
0 2005-01-05 15:00:37 PST by root via cli commit confirmed, rollback in 3mins

```

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 410 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 410](#)
  - [Committing a Junos OS Configuration on page 406](#)

## 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 406](#)
- [Monitoring the Junos Commit Process on page 411](#)

## 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 406](#)
- [Adding a Comment to Describe the Committed Configuration on page 412](#)

## 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 406](#)
- [Backing Up the Committed Configuration on the Alternate Boot Drive on page 413](#)

## Backing Up the Committed Configuration on the Alternate Boot Drive

After you commit the configuration and are satisfied that it is running successfully, you should issue the **request system snapshot** command to back up the new software onto the **/altconfig** file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The **request system snapshot** command backs up the root file system to **/altroot**, and **/config** to **/altconfig**. The root and **/config** file systems are on the router's flash drive, and the **/altroot** and **/altconfig** file systems are on the router's hard disk (if available).



**NOTE:** To back up the file system on a J Series Services Router, you must specify a media type (primary compact flash drive, removable compact flash drive, or USB storage device) for backup. For more information about the **request system snapshot** command, see [CLI Explorer](#).

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 406](#)

## Example: Configuring Junos OS Batch Commits

- [Junos OS Batch Commits Overview on page 414](#)
- [Example: Configuring Batch Commit Server Properties on page 414](#)

### 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 415](#)
- [Overview on page 415](#)



- [Configuration on page 415](#)
- [Verification on page 417](#)

### 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 417](#)
- [Checking the Batch Commit Status on page 417](#)
- [Viewing the Patch Files in a Batch Commit Job on page 418](#)
- [Viewing the Trace Files for Batch Commit Operations on page 420](#)

### 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
...
```

## Loading a Junos OS Configuration

- [Loading a Configuration from a File on page 421](#)
- [Examples: Loading a Configuration from a File on page 424](#)

### 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 500](#).

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>
```

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 424](#).

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 424](#).

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 424](#).

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 425](#).



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 425](#).

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 424](#)

## Examples: Loading a Configuration from a File

Figure 15: Overriding the Current Configuration

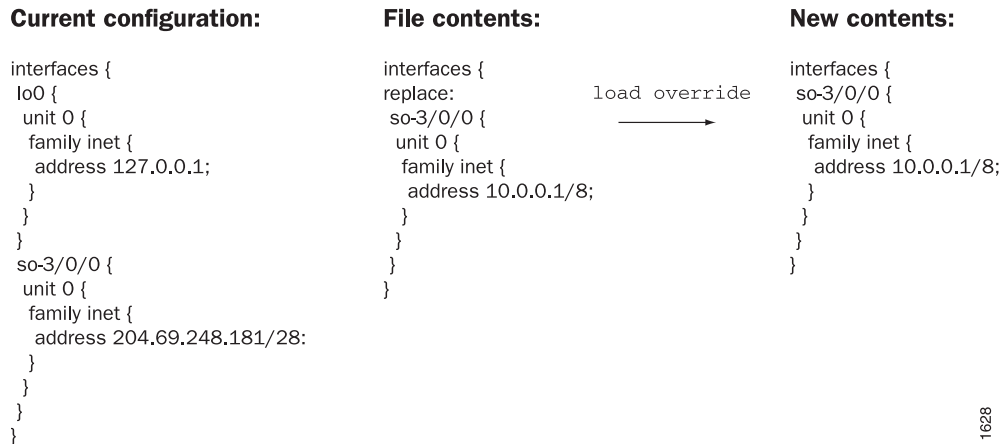


Figure 16: Using the replace Option

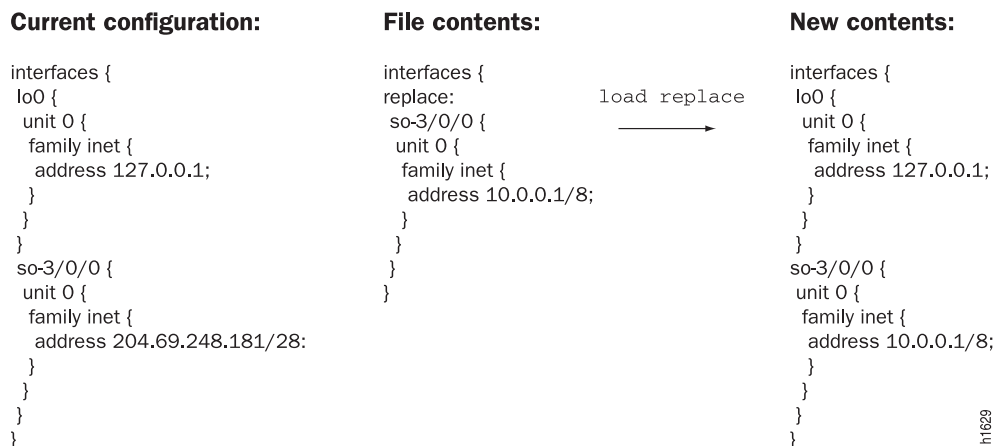


Figure 17: Using the merge Option

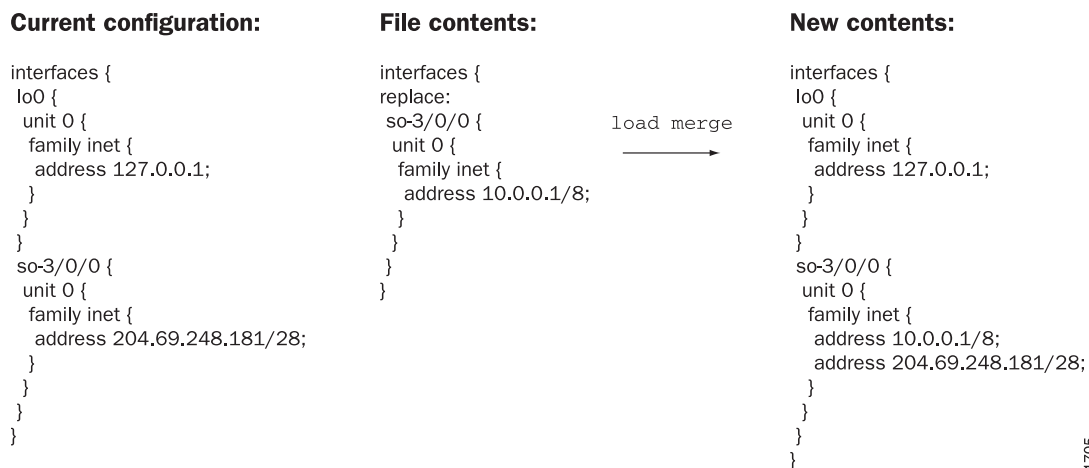


Figure 18: Using a Patch File

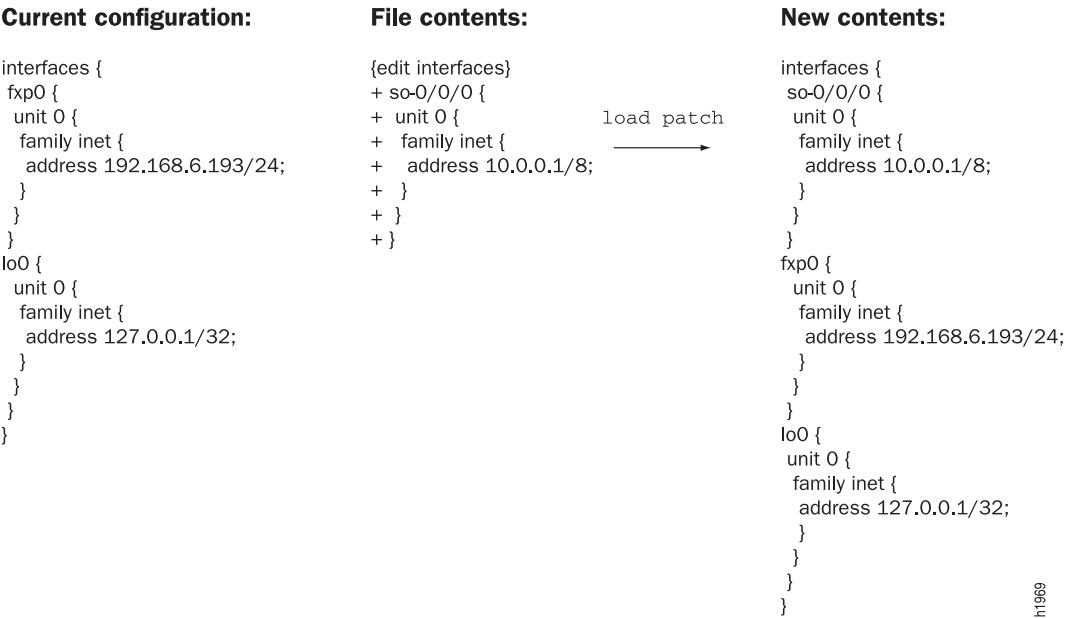


Figure 19: Using the set Option



Related Documentation

- [Loading a Configuration from a File on page 421](#)

## Synchronizing the Junos OS Configuration

- [Synchronizing Routing Engines on page 426](#)

### 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 429](#).

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. .

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.

## Creating and Applying Junos OS Configuration Groups

- [Creating a Junos Configuration Group on page 428](#)
- [Applying a Junos Configuration Group on page 429](#)
- [Example: Configuring and Applying Junos Configuration Groups on page 431](#)
- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 432](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 433](#)
- [Using Wildcards with Configuration Groups on page 435](#)
- [Example: Using Conditions to Apply Configuration Groups on page 438](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 440](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 442](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 444](#)
- [Example: Configuring Peer Entities on page 445](#)
- [Establishing Regional Configurations on page 447](#)

- [Selecting Wildcard Names on page 448](#)
- [Using Junos OS Defaults Groups on page 450](#)
- [Example: Referencing the Preset Statement From the Junos defaults Group on page 451](#)
- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 452](#)

## 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 450](#).

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 429](#).

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..



**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 429](#)
- [Using Junos OS Defaults Groups on page 450](#)
- [Understanding the Junos Configuration Groups on page 353](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 433](#)
- [Using Wildcards with Configuration Groups on page 435](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 440](#)

## 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 431](#)
- [Disabling Inheritance of a Junos OS Configuration Group on page 433](#)



- [Creating a Junos Configuration Group on page 428](#)
- [Using Wildcards with Configuration Groups on page 435](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 440](#)

## 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.

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 433](#).

### Related Documentation

- [Example: Creating and Applying Configuration Groups on a TX Matrix Router on page 432](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 442](#)
- [Example: Configuring Peer Entities on page 445](#)
- [Example: Referencing the Preset Statement From the Junos defaults Group on page 451](#)

- [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 452](#)
- [Example : Configuring Sets of Statements with Configuration Groups on page 440](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 444](#)
- [Creating a Junos Configuration Group on page 428](#)

## 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 {
```

**Related Documentation**

- [Example: Configuring and Applying Junos Configuration Groups on page 431](#)
- [Creating a Junos Configuration Group on page 428](#)

To disable inheritance of a configuration group at any level except the top level of the hierarchy, include the **apply-groups-except** statement:

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.

```
[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 429](#).

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 429](#)
- [Understanding the Junos Configuration Groups on page 353](#)

## 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 448](#)
- [Applying a Junos Configuration Group on page 429](#)
- [Creating a Junos Configuration Group on page 428](#)
- [Understanding the Junos Configuration Groups on page 353](#)

## Example: Using Conditions to Apply Configuration Groups

- [Using Conditions to Apply Configuration Groups Overview on page 438](#)
- [Example: Configuring Conditions for Applying Configuration Groups on page 438](#)

### 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.

### 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 438](#)
- [Overview on page 438](#)
- [Configuration on page 439](#)

#### **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. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

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 440](#)

#### **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 353](#)
  - [Creating a Junos Configuration Group on page 428](#)
  - [Applying a Junos Configuration Group on page 429](#)

## **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 353](#)
- [Creating a Junos Configuration Group on page 428](#)
- [Applying a Junos Configuration Group on page 429](#)

### 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 353](#)
- [Creating a Junos Configuration Group on page 428](#)
- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 493](#)
- [Example: Configuring a Consistent IP Address for the Management Interface on page 444](#)

### Example: Configuring a Consistent IP Address for the Management Interface

On routers with multiple Routing Engines, each Routing Engine is configured with a separate IP address for the management interface (**fxp0**). To access the master Routing Engine, you must know which Routing Engine is active and use the appropriate IP address.

Optionally, for consistent access to the master Routing Engine, you can configure an additional IP address and use this address for the management interface regardless of which Routing Engine is active. This additional IP address is active only on the management interface for the master Routing Engine. During switchover, the address moves to the new master Routing Engine.

In the following example, address **10.17.40.131** is configured for both Routing Engines and includes a **master-only** statement. With this configuration, the **10.17.40.131** address is active only on the master Routing Engine. The address remains consistent regardless of which Routing Engine is active. Address **10.17.40.132** is assigned to **fxp0** on **re0**, and **10.17.40.133** is assigned to **fxp0** on **re1**.

```

[edit groups re0 interfaces fxp0]
unit 0 {
    family inet {
        address 10.17.40.131/25 {
            master-only;
        }
        address 10.17.40.132/25;
    }
}
[edit groups re1 interfaces fxp0]

```

```

unit 0 {
  family inet {
    address 10.17.40.131/25 {
      master-only;
    }
    address 10.17.40.133/25;
  }
}

```

This feature is available on all routers that include dual Routing Engines. On a routing matrix composed of the TX Matrix router, this feature is applicable to the switch-card chassis (SCC) only. Likewise, on a routing matrix composed of a TX Matrix Plus router, this feature is applicable to the switch-fabric chassis (SFC) only.



#### NOTE:

- If you configure the same IP address for a management interface or internal interface such as `fxp0` and an external physical interface such as `ge-0/0/1`, when graceful Routing Engine switchover (GRES) is enabled, the CLI displays an appropriate commit error message that identical addresses have been found on the private and public interfaces. In such cases, you must assign unique IP addresses for the two interfaces that have duplicate addresses.
- The management Ethernet interface used for the TX Matrix Plus router, T1600 routers in a routing matrix, and PTX Series Packet Transport Switches, is `em0`. Junos OS automatically creates the router's management Ethernet interface, `em0`.

#### Related Documentation

- [Understanding the Junos Configuration Groups on page 353](#)
- [Creating a Junos Configuration Group on page 428](#)
- [Example: Configuring Interfaces Using Junos OS Configuration Groups on page 442](#)

## 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 353](#)
  - [Creating a Junos Configuration Group on page 428](#)
  - [Establishing Regional Configurations on page 447](#)

## 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 353](#)
  - [Example: Configuring Peer Entities on page 445](#)

## 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;
                }
            }
        }
    }
}

```



**Related Documentation** • [Using Wildcards with Configuration Groups on page 435](#)

## 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 428](#)
  - [Example: Referencing the Preset Statement From the Junos defaults Group on page 451](#)
  - [Example: Viewing Default Statements That Have Been Applied to the Configuration on page 452](#)

### 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 452](#)
  - [Using Junos OS Defaults Groups on page 450](#)
  - [Understanding the Junos Configuration Groups on page 353](#)
  - [Creating a Junos Configuration Group on page 428](#)

## 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 428](#)
  - [Configuring Configuration Groups on page 354](#)

---

## CLI Online Help

- [Examples: Using Command Completion in Configuration Mode on page 452](#)
- [Examples: Using the Junos OS CLI Command Completion on page 454](#)
- [Displaying the Junos OS CLI Command and Word History on page 455](#)

## 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
  lo0only-v4        Name to identify a policy filter
  lo0only-v6        Name to identify a policy filter
  lo2bgp            Name to identify a policy filter
```

#### Related Documentation

- [Examples: Using the Junos OS CLI Command Completion on page 454](#)
- [Displaying the Junos OS CLI Command and Word History on page 455](#)

## Examples: Using the Junos OS CLI Command Completion

The following examples show how you can use the command completion feature in Junos OS. Issue the **show interfaces** command:

```
user@host> sh<Space>ow i<Space>
'i' is ambiguous.
Possible completions:
igmp          Show information about IGMP
interface     Show interface information
isis          Show information about IS-IS

user@host> show in<Space>terfaces
Physical interface: at-0/1/0, Enabled, Physical link is Up
Interface index: 11, SNMP ifIndex: 65
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode
Speed: OC12, Loopback: None, Payload scrambler: Enabled
Device flags: Present Running
Link flags: 0x01
...
```

```
user@host>
```

Display a list of all log files whose names start with the string “messages,” and then display the contents of one of the files:

```
user@myhost> show log mes?
Possible completions:
  <filename>Log file to display
messagesSize: 1417052, Last changed: Mar 3 00:33
messages.0.gzSize: 145575, Last changed: Mar 3 00:00
messages.1.gzSize: 134253, Last changed: Mar 2 23:00
messages.10.gzSize: 137022, Last changed: Mar 2 14:00
messages.2.grSize: 137112, Last changed: Mar 2 22:00
messages.3.gzSize: 121633, Last changed: Mar 2 21:00
messages.4.gzSize: 135715, Last changed: Mar 2 20:00
messages.5.gzSize: 137504, Last changed: Mar 2 19:00
messages.6.gzSize: 134591, Last changed: Mar 2 18:00
messages.7.gzSize: 132670, Last changed: Mar 2 17:00
messages.8.gzSize: 136596, Last changed: Mar 2 16:00
messages.9.gzSize: 136210, Last changed: Mar 2 15:00

user@myhost> show log mes<Tab>sages.4<Tab>.gz<Enter>
Jan 15 21:00:00 myhost newsyslog[1381]: logfile turned over
...
```



- Related Documentation**
- [Displaying the Junos OS CLI Command and Word History on page 455](#)

## Displaying the Junos OS CLI Command and Word History

To display a list of recent commands that you issued, use the **show cli history** command:

```
user@host> show cli history 3
01:01:44 -- show bgp next-hop-database
01:01:51 -- show cli history
01:02:51 -- show cli history 3
```

You can press Esc+. (period) or Alt+. (period) to insert the last word of the previous command. Repeat Esc+. or Alt+. to scroll backwards through the list of recently entered words. For example:

```
user@host> show interfaces terse fe-0/0/0
Interface      Admin    Link    Proto    Local    Remote
fe-0/0/0       up      up      inet     192.168.220.1/30
fe-0/0/0.0     up      up      inet     192.168.220.1/30

user@host> <Esc>
user@host> fe-0/0/0
```

If you scroll completely to the beginning of the list, pressing Esc+. or Alt+. again restarts scrolling from the last word entered.

- Related Documentation**
- [Junos OS CLI Online Help Features on page 317](#)

## CLI Configuration Mode

- [Example: Using the configure Command on page 455](#)

### 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 342](#)

---

## Controlling the CLI Environment

- [Example: Controlling the CLI Environment on page 456](#)

### 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 514](#)
  - [Controlling the Junos OS CLI Environment on page 509](#)

---

## CLI Advanced Features

- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 456](#)
- [Example: Using Global Replace in a Junos Configuration—Replacing an Interface Name on page 457](#)
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 458](#)

### 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 457](#)
  - [Using Global Replace in a Junos Configuration on page 349](#)

## 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

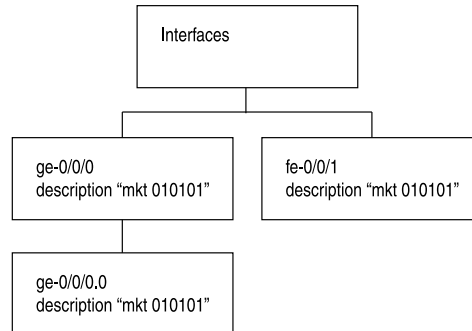
- [Example: Using Global Replace in a Junos Configuration—Using the upto Option on page 458](#)
- [Using Global Replace in a Junos Configuration on page 349](#)

### Example: Using Global Replace in a Junos Configuration—Using the upto Option

Consider the hierarchy shown in [Figure 20 on page 458](#). 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:

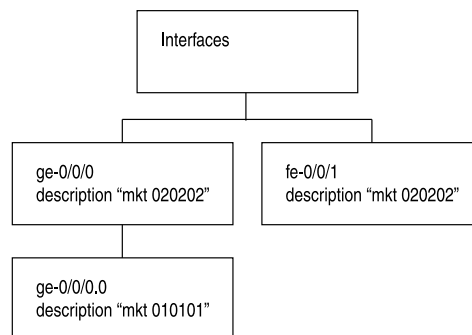
**Figure 20: Replacement by Object**

Current Configuration:



user@host > **replace pattern 01 with pattern 02 upto 2**

Resulting Configuration:



g017228

An **upto 2** option in the **replace** command converts **01** to **02** for two object instances. The objects under the main interfaces **ge-0/0/0** and **fe-0/0/1** will be replaced first (since these are siblings in the hierarchy level). Because of the **upto 2** restriction, the **replace** command replaces patterns in the first and second instance in the hierarchy (siblings), but not the third instance (child of the first instance).

```

user@host# show interfaces
ge-0/0/0 {
  description "mkt 010101"; #First instance in the hierarchy
  unit 0 {
    description "mkt 010101"; #Third instance in the hierarchy (child of the first
    instance)
  }
}
fe-0/0/1 {
  description "mkt 010101"; #second instance in the hierarchy (sibling of the first
  instance)
  unit 0 {
    family inet {
      address 200.200.20.2/24;
    }
  }
}
[edit]
user@host# replace pattern 01 with 02 upto 2
[edit]
user@host# commit
commit complete

[edit]
user@host# show interfaces
ge-0/0/0 {
  description "mkt 020202"; #First instance in the hierarchy
  unit 0 {
    description "mkt 010101"; #Third instance in the hierarchy (child of the first
    instance)
  }
}
fe-0/0/1 {
  description "mkt 020202"; #second instance in the hierarchy (sibling of the first
  instance)
  unit 0 {
    family inet {
      address 200.200.20.2/24;
    }
  }
}

```

#### Related Documentation

- [Using Global Replace in a Junos Configuration on page 349](#)

## Configuration Statements

---

- [apply-groups](#) on page 461
- [apply-groups-except](#) on page 461
- [commit-interval](#) (Batch Commits) on page 462
- [groups](#) on page 463
- [days-to-keep-error-logs](#) (Batch Commits) on page 465
- [deactivate](#)
- [delete](#)
- [edit](#)
- [exit](#)
- [help](#)
- [insert](#)
- [load](#)
- [maximum-aggregate-pool](#) (Batch Commits) on page 473
- [maximum-entries](#) (Batch Commits) on page 474
- [protect](#)
- [quit](#)
- [rename](#)
- [rename](#)
- [replace](#)
- [rollback](#)
- [run](#)
- [save](#)
- [server](#) (Batch Commits) on page 483
- [set](#)
- [status](#)
- [top](#)
- [traceoptions](#) (Batch Commits) on page 487
- [unprotect](#)
- [up](#)
- [update](#)
- [when](#) on page 491
- [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 429</a></li> <li>• <a href="#">groups on page 463</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 463</a></li> <li>• <a href="#">Disabling Inheritance of a Junos OS Configuration Group on page 433</a></li> </ul>

## commit-interval (Batch Commits)

---

<b>Syntax</b>	commit-interval <i>number-of-seconds-between-commits</i> ;
<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>	<i>number-of-seconds-between-commits</i> —Time interval (in seconds) between two commit operations. <b>Range:</b> 1 through 30 seconds. <b>Default:</b> 5 seconds.
<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="#">Example: Configuring Junos OS Batch Commits on page 414</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 428](#)
  - [apply-groups on page 461](#)
  - [apply-groups-except on page 461](#)

---

## days-to-keep-error-logs (Batch Commits)

---

<b>Syntax</b>	<code>days-to-keep-error-logs</code> <i>days-to-keep-error-log-entries</i> ;
<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>	<i>days-to-keep-error-log-entries</i> —Number of days to keep the error logs. <b>Range:</b> 1 through 366 days <b>Default:</b> 1 day
<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="#">Example: Configuring Junos OS Batch Commits on page 414</a></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 535</a></li><li>• <a href="#">delete on page 467</a></li><li>• <a href="#">Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 388.</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 466</a></li> <li>• <a href="#">Deleting a Statement from a Junos Configuration on page 382</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 484</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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 486</a></li><li>• <a href="#">up on page 489</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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>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 315</a></li></ul>



---

## insert

---

<b>Syntax</b>	insert < <i>statement-path</i> > <i>identifier1</i> (before   after) <i>identifier2</i>
<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 386</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>On J Series Services Routers, pressing and holding down the Config button on the router for 15 seconds causes the factory configuration to be loaded and committed. However, this operation deletes all other configurations on the router; using the <b>load factory-default</b> command does not.</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 500</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*.

**Required Privilege Level** configure—To enter configuration mode, but other required privilege levels depend on where the statement is located in the configuration hierarchy.

**Related Documentation**

- [Loading a Configuration from a File on page 421](#)

## maximum-aggregate-pool (Batch Commits)

**Syntax** maximum-aggregate-pool *maximum-number-of-commits-to-aggregate*;

**Hierarchy Level** [edit system commit server]

**Release Information** Statement introduced in Junos OS Release 12.1.

**Description** For Junos OS batch commits, specify the maximum number of individual commit operations that are aggregated or merged into a single commit operation.

**Options** *maximum-number-of-commits-to-aggregate*—Maximum number of individual commit operations that are aggregated or merged into a single commit operation.

**Range:** 1 through 4294967295

**Default:** 5

**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 on page 414](#)

## 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>• <a href="#">Example: Configuring Junos OS Batch Commits on page 414</a></li></ul>

## protect

---

<b>Syntax</b>	<code>protect (hierarchy   statement   identifier)</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 399</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 486</a></li><li>• <a href="#">up on page 489</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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 385](#)

## 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 385](#)



## 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 349</a></li> </ul>

## rollback

---

<b>Syntax</b>	<code>rollback &lt;number   rescue&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>	<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>none (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 569</a></li><li>• <a href="#">Creating and Returning to a Rescue Configuration on page 573</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 334</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 388](#)

## 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 on page 414](#)

## set

---

<b>Syntax</b>	set < <i>statement-path</i> > <i>identifier</i>
<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 468</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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 364.</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 360</a></li><li>• <a href="#">exit on page 469</a></li><li>• <a href="#">up on page 489</a></li></ul>



## traceoptions (Batch Commits)

<b>Syntax</b>	<pre> traceoptions {     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 traceoptions 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>• <a href="#">Example: Configuring Junos OS Batch Commits on page 414</a></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 486</a></li><li>• <a href="#">up on page 489</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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 360</a></li><li>• <a href="#">exit on page 469</a></li><li>• <a href="#">top on page 486</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 on page 368.](#)

## 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 428</a></li> <li>• <a href="#">apply-groups on page 461</a></li> <li>• <a href="#">apply-groups-except on page 461</a></li> <li>• <a href="#">groups on page 463</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 458.</a></li></ul>

## CHAPTER 10

# Administration

- [CLI Operational Mode on page 493](#)
- [Routine Monitoring on page 495](#)
- [Managing the CLI Environment on page 509](#)
- [CLI Advanced Features on page 515](#)
- [Junos OS CLI Environment Commands on page 517](#)
- [Operational Commands on page 532](#)

### CLI Operational Mode

---

- [Interface Naming Conventions Used in the Junos OS Operational Commands on page 493](#)

### 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 493](#)
- [Logical Part of an Interface Name on page 494](#)
- [Channel Identifier Part of an Interface Name on page 494](#)

#### 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 J Series Services Routers and 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.

- J Series and SRX interface names—On J Series and SRX devices, the unique name of each network interface has the following format to identify the physical device that corresponds to a single physical network connector:

*type-slot/pim-or-ioc/port*

For more information about J Series and SRX interface naming conventions, see the *Junos OS Interfaces Library 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*

- J Series and 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 *Junos OS Interfaces Library 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*

- J Series and 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 442](#)

## Routine Monitoring

- [Checking the Status of a Device Running Junos OS on page 495](#)
- [Monitoring Who Uses the Junos OS CLI on page 497](#)
- [Viewing Files and Directories on a Device Running Junos OS on page 497](#)
- [Displaying Junos OS Information on page 501](#)
- [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 503](#)
- [Using the Junos OS CLI Comment Character # for Operational Mode Commands on page 508](#)
- [Example: Using Comments in Junos OS Operational Mode Commands on page 508](#)

## 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 455](#)
  - [Managing Programs and Processes Using Junos OS Operational Mode Commands on page 503](#)
  - [Viewing Files and Directories on a Device Running Junos OS on page 497](#)

## 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 358](#)
  - [Controlling the Junos OS CLI Environment on page 509](#)

## 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 498](#)
- [Listing Files and Directories on page 498](#)
- [Specifying Filenames and URLs on page 500](#)

## Directories on the Router or Switch

Table 49 on page 498 lists some standard directories on a device running Junos OS.

**Table 49: 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 <b>/config</b> 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 501](#)

## 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 503](#)

## 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 504](#)
- [Restarting a Junos OS Process on page 505](#)
- [Stopping the Junos OS on page 506](#)
- [Rebooting the Junos OS on page 507](#)

## 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	vluwt	0:26	0.00%	0.00%	vntru
3371	root	2	0	1024K	216K	sbwait	0:25	0.00%	0.00%	tnp.sntpd
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%	l2cpd
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 50 on page 505 lists and describes the output fields included in this example. The fields are listed in alphabetical order.

**Table 50: 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 21 on page 506.](#))

Figure 21: Restarting a Process

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	CPU	COMMAND
546	root	10	0	9096K	1720K	nanslp	0:21	0.00%	0.00%	chassisd
685	root	2	0	12716K	3840K	kqread	0:01	0.00%	0.00%	rpdp
553	root	2	0	8792K	1544K	select	0:01	0.00%	0.00%	mib2d

PID before restart

547	root	2	0	7732K	888K	select	0:00	0.00%	0.00%	alarmd
545	root	2	0	10292K	2268K	select	0:00	0.00%	0.00%	dcd
1	root	10	0	816K	520K	wait	0:00	0.00%	0.00%	init
550	root	2	-12	1308K	692K	select	0:00	0.00%	0.00%	ntpd
758	root	32	0	21716K	832K	RUN	0:00	0.00%	0.00%	top
560	root	2	0	8208K	1088K	select	0:00	0.00%	0.00%	rmopd
561	root	2	0	8188K	1156K	select	0:00	0.00%	0.00%	cosd
559	root	2	0	1632K	840K	select	0:00	0.00%	0.00%	ilmid
573	lab	2	0	7480K	2580K	select	0:00	0.00%	0.00%	cli
751	root	2	0	12716K	3944K	kqread	0:00	0.00%	0.00%	rpdp
558	root	2	20	8708K	1880K	select	0:00	0.00%	0.00%	sampd
555	root	2	0	1856K	932K	select	0:00	0.00%	0.00%	vrpd
686	root	2	0	7808K	940K	select	0:00	0.00%	0.00%	apd

PID after restart

## 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 495](#)
  - [Displaying Junos OS Information on page 501](#)

## 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 508](#)

### 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 508](#)

## Managing the CLI Environment

- [Controlling the Junos OS CLI Environment on page 509](#)
- [Overview of Junos OS CLI Operational Mode Commands on page 512](#)
- [Setting the Junos OS CLI Screen Length and Width on page 514](#)

### 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 510](#)
- [Setting the CLI Prompt on page 510](#)
- [Setting the CLI Directory on page 510](#)
- [Setting the CLI Timestamp on page 510](#)
- [Setting the Idle Timeout on page 511](#)
- [Setting the CLI to Prompt After a Software Upgrade on page 511](#)
- [Setting Command Completion on page 511](#)
- [Displaying CLI Settings on page 511](#)

---

### 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 456](#)

## 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 512](#)
- [Commonly Used Operational Mode Commands on page 513](#)

### 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 311](#).
- 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 334.
- A command—**quit**—to exit the CLI. For information about this command, see [CLI Explorer](#).

### Commonly Used Operational Mode Commands

Table 41 on page 320 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 51: 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>

Table 51: Commonly Used Operational Mode Commands (*continued*)

Items to Check	Description	Command
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>
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 322](#)
- [Understanding the Brief, Detail, Extensive, and Terse Options of Junos OS Operational Commands on page 322](#)

## 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 514](#)
- [Setting the Screen Width on page 515](#)
- [Understanding the Screen Length and Width Settings on page 515](#)

### 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 456](#)
- [Controlling the Junos OS CLI Environment on page 509](#)

## CLI Advanced Features

- [Common Regular Expressions to Use with the replace Command on page 516](#)

## Common Regular Expressions to Use with the replace Command

**Table 52: 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 53 on page 516 lists some replacement examples.

**Table 53: Replacement Examples**

Command	Result
replace pattern myrouter with router1	Match: myrouter Result: router1
replace pattern "192.168\.(*)/24" with "10.2.\1/28"	Match: 192.168.3.4/24 Result: 10.2.3.4/28
replace pattern "1.\1" with "abc&def"	Match: 1.1 Result: abc1.1def

Table 53: Replacement Examples (*continued*)

Command	Result
<code>replace pattern 1.1 with " abc\&amp;def"</code>	Match: 1#1 Result: <code>abc&amp;def</code>

**Related  
Documentation**

- [Using Global Replace in a Junos Configuration on page 349](#)
- [Example: Using Global Replace in a Junos Configuration—Using the \n Back Reference on page 456](#)

## 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 528</a></li></ul>
<b>List of Sample Output</b>	<a href="#">set cli complete-on-space on page 518</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 519</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 520</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 510</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 511</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 514</a></li><li>• <a href="#">Understanding the Screen Length and Width Settings on page 515</a></li><li>• <a href="#">set cli screen-width on page 524</a></li><li>• <a href="#">set cli terminal on page 525</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 515</a></li><li>• <a href="#">set cli screen-length on page 523</a></li><li>• <a href="#">set cli terminal on page 525</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 510</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 510</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 528</a>
<b>Output Fields</b>	<a href="#">Table 54 on page 528</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 54: 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>	show cli history < <i>count</i> >
<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 455</a></li></ul>

## Operational Commands

---

- | (pipe)
- activate
- annotate
- commit
- configure
- copy
- file
- help
- 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

## | (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>Junos OS Configuration and Operations Automation Library</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 332](#).

**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 500](#).

**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 360](#).
- [Using the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)
- [Using Regular Expressions with the Pipe \( | \) Symbol to Filter Junos Command Output on page 327](#)
- [Pipe \( | \) Filter Functions in the Junos OS command-line interface on page 328](#)



---

## 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 466</a></li><li>• <a href="#">Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 388</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 oneliner) 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 390](#)

## 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 433](#).

The responding Routing Engine must use Junos OS Release 5.0 or later.

**Required Privilege Level**

`configure`—To enter configuration mode.



**NOTE:** If you are using Junos OS in a Common Criteria environment, system log messages are created whenever a secret attribute is changed (for example, password changes or changes to the RADIUS shared secret). These changes are logged during the following configuration load operations:

```
load merge
load replace
load override
load update
```

For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*

**Related Documentation**

- [Verifying a Junos Configuration on page 399](#), [Committing a Junos OS Configuration on page 406](#)
- [Scheduling a Junos Commit Operation on page 410](#)
- [Deactivating and Reactivating Statements and Identifiers in a Junos Configuration on page 388](#)
- [Monitoring the Junos Commit Process on page 411](#)
- [Adding a Comment to Describe the Committed Configuration on page 412](#)

## configure

<b>Syntax</b>	configure <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>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 559</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">configure on page 540</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 384</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 497</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 315</a></li></ul>

## 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 319](#)

## restart

**List of Syntax**    [Syntax on page 547](#)

[Syntax \(EX Series Switches\) on page 547](#)

[Syntax \(TX Matrix Routers\) on page 547](#)

[Syntax \(TX Matrix Plus Routers\) on page 548](#)

[Syntax \(MX Series Routers\) on page 548](#)

[Syntax \(J Series Routers\) on page 548](#)

[Syntax \(QFX Series\) on page 548](#)

**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 (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>
<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)	<pre>restart &lt;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 &lt;logical-system <i>logical-system-name</i>&gt;   sampling   service-deployment   snmp   statistics-service&gt; &lt;all-chassis   all-lcc   all-sfc   lcc <i>number</i>   sfc <i>number</i>&gt; &lt;gracefully   immediately   soft&gt;</pre>
Syntax (MX Series Routers)	<pre>restart &lt;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 &lt;logical-system <i>logical-system-name</i>&gt;   sampling   sbc-configuration-process   sdk-service   service-deployment   services   services pgcp gateway <i>gateway-name</i>   snmp   soft   static-subscribers   statistics-service   subscriber-management   subscriber-management-helper   tunnel-oamd   usb-control   vrrp   web-management&gt; &lt;all-members&gt; &lt;gracefully   immediately   soft&gt; &lt;local&gt; &lt;member <i>member-id</i>&gt;</pre>
Syntax (J Series Routers)	<pre>restart &lt;adaptive-services   audit-process   chassis-control   class-of-service   dhcp   dhcp-service   dialer-services   diameter-service   event-processing   firewall   interface-control   ipsec-key-management   isdn-signaling   l2ald   l2-learning   l2tp-service   mib-process   network-access-service   pgm   ppp   pppoe   remote-operations   routing &lt;logical-system <i>logical-system-name</i>&gt;   sampling   service-deployment   snmp   usb-control   web-management&gt; &lt;gracefully   immediately   soft&gt;</pre>
Syntax (QFX Series)	<pre>restart &lt;adaptive-services   audit-process   chassis-control   class-of-service   dialer-services   diameter-service   dlsd   ethernet-connectivity   event-processing   fibre-channel   firewall   general-authentication-service   igmp-host-services   interface-control   ipsec-key-management   isdn-signaling   l2ald   l2-learning   l2tp-service   mib-process   named-service   network-access-service   nstrace-process   pgm   ppp   pppoe   redundancy-interface-process   remote-operations   <i>logical-system-name</i>&gt;   routing   sampling   secure-neighbor-discovery   service-deployment   snmp   usb-control   web-management&gt; &lt;gracefully   immediately   soft&gt;</pre>

**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.  
 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 upon 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**—(J Series routers and 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**—(J Series routers and 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.



**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**—(J Series routers and 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) (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 router) (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) (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**—(J Series routers and 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**—(J Series routers and MX Series routers) (Optional) Restart the USB control process.

**vrrp**—(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**—(J Series routers, 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 319](#)

**List of Sample Output**    [restart interfaces on page 556](#)

**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>	set < <i>statement-path</i> > <i>identifier</i>
<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 468</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</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><code>identifier</code>—(Optional) Display the configuration for the specified identifier.</p> <p><code>statement-path</code>—(Optional) Display the configuration for the specified statement hierarchy path.</p>
<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 562</a></li><li>• <a href="#">show   display omit on page 563</a></li><li>• <a href="#">show   display set on page 564</a></li><li>• <a href="#">show   display set relative on page 565</a></li><li>• <a href="#">show groups junos-defaults on page 566</a></li><li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</a></li></ul>



## show configuration

---

<b>Syntax</b>	show configuration < <i>statement-path</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>	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><i>statement-path</i></b>—(Optional) Display one of the following hierarchies in a configuration. (Each <b><i>statement-path</i></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.

<b>Additional Information</b>	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 <b>ACCESS-DENIED</b> 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 <b>secret</b> permission bit is not set for your user account, the text <b>SECRET-DATA</b> is substituted for that portion of the configuration. If an identifier in the configuration contains a space, the identifier is displayed in quotation marks.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Displaying the Current Junos OS Configuration on page 360</a></li> <li>• <a href="#">Overview of Junos OS CLI Operational Mode Commands on page 319</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show configuration on page 560</a> <a href="#">show configuration policy-options on page 561</a>
<b>Output Fields</b>	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 "8.2I0 [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 450](#)

---

## show | display omit

---

<b>Syntax</b>	show   display omit
<b>Release Information</b>	Command introduced in Junos OS Release 8.2.
<b>Description</b>	<p>Display configuration statements (including those marked as hidden by the <b>apply-flags omit</b> configuration statement).</p> <pre>user@host# show   display omit system {   apply-flags omit;   login {     message lengthy-login-message;   } }</pre>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show on page 558</a></li></ul>

## show | display set

---

**Syntax**    show | display set

**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 top level of the hierarchy as **set** commands

```
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
```

**Required Privilege Level**    view

- Related Documentation**
- [show on page 558](#)
  - [Displaying set Commands from the Junos OS Configuration on page 361](#)

## show | display set relative

<b>Syntax</b>	show   display set relative
<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 current hierarchy level.</p> <pre>[edit interfaces fe-0/0/0] user@host# show unit 0 {   family inet {     address 192.107.1.230/24;   }   family iso;   family mpls; } inactive: unit 1 {   family inet {     address 10.0.0.1/8;   } } user@host# show   display set relative set unit 0 family inet address 192.107.1.230/24 set unit 0 family iso set unit 0 family mpls set unit 1 family inet address 10.0.0.1/8 deactivate unit 1</pre>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Displaying set Commands from the Junos OS Configuration on page 361</a></li> </ul>

## 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 450](#)
- *Junos OS UTM Library for Security Devices*



## 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 pending commit operation (if any) and the commit history.
<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 568</a> <a href="#">show system commit (At a Particular Time) on page 568</a> <a href="#">show system commit (At the Next Reboot) on page 568</a> <a href="#">show system commit (Rollback Pending) on page 568</a> <a href="#">show system commit (QFX Series) on page 568</a>
<b>Output Fields</b>	Table 55 on page 567 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 55: 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>—A method other than those identified was used to perform the commit operation.</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
```

# Troubleshooting

- [Troubleshooting Procedures on page 569](#)

## Troubleshooting Procedures

---

- [Returning to the Most Recently Committed Junos Configuration on page 569](#)
- [Returning to a Previously Committed Junos OS Configuration on page 569](#)
- [Creating and Returning to a Rescue Configuration on page 574](#)
- [Rolling Back Junos OS Configuration Changes on page 575](#)

### 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 575](#)
- [Returning to a Previously Committed Junos OS Configuration on page 569](#)
- [Understanding How the Junos Configuration Is Stored on page 354](#)

### 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 570](#)
- [Displaying Previous Configurations on page 570](#)

- [Comparing Configuration Changes with a Prior Version on page 571](#)
- [Creating and Returning to a Rescue Configuration on page 573](#)
- [Saving a Configuration to a File on page 573](#)

---

### 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 569](#)
- [Loading a Configuration from a File on page 421](#)
- [Specifying Filenames and URLs on page 500](#)

## 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 571](#)
- [Saving a Configuration to a File on page 573](#)

## 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 569](#)

## PART 4

# J-Web User Guide

- [Overview on page 579](#)
- [Configuration on page 593](#)
- [Administration on page 611](#)
- [Troubleshooting on page 651](#)



## CHAPTER 12

# Overview

- [J-Web User Interface on page 579](#)
- [Installation and Setup on page 585](#)
- [Secure Web Access on page 591](#)

### J-Web User Interface

---

- [J-Web Overview on page 579](#)
- [J-Web Layout on page 580](#)
- [Top Pane Elements on page 580](#)
- [Main Pane Elements on page 581](#)
- [Side Pane Elements on page 582](#)
- [Navigating the J-Web Interface on page 583](#)
- [Navigating the J-Web Configuration Editor on page 584](#)
- [Getting J-Web Help on page 584](#)

### J-Web Overview

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI.

You can perform the following tasks with the J-Web interface:

- **Monitoring**—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- **Configuring**—View the current configurations at a glance, configure the routing platform, and manage configuration files. The J-Web interface provides the following different configuration methods:
  - Configure the routing platform quickly and easily without configuring each statement individually.
  - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.

- Edit the configuration in a text file.
- Upload a configuration file.

The J-Web interface also allows you to manage configuration history and set a rescue configuration.

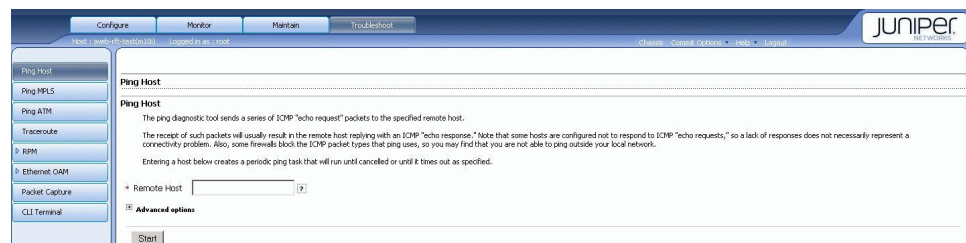
- Troubleshooting—Troubleshoot routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic.
- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms. On J Series routers, you can also manage software packages and licenses and copy a snapshot of the system software to a backup device.
- 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.
- Configuring and monitoring alarms—On J Series routers only, monitor and diagnose the router 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.

## J-Web Layout

Each page of the J-Web interface is divided into the following panes, as shown in [Figure 22 on page 580](#).

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, troubleshoot, and manage the routing platform 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.

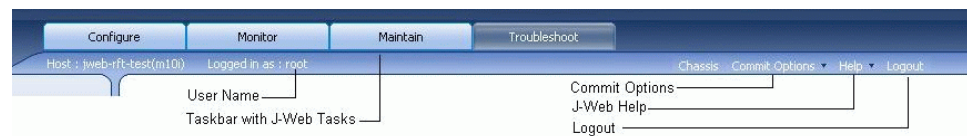
**Figure 22: J-Web Layout**



## Top Pane Elements

The top pane comprises the elements shown in [Figure 23 on page 581](#).

Figure 23: Top Pane Elements



- *hostname – model*—Hostname and model of the routing platform.
- Logged in as: *username*—Username you used to log in to the routing platform.
- 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 routing platform and returns you to the login page.
- Taskbar—Menu of J-Web tasks. Click a J-Web task to access it.
  - **Configure**—Configure the routing platform by using Configuration pages or the configuration editor, and view configuration history.
  - **Monitor**—View information about configuration and hardware on the routing platform.
  - **Maintain**—Manage files and licenses, upgrade software, and reboot the routing platform.
  - **Troubleshoot**—Troubleshoot network connectivity problems.

## Main Pane Elements

The main pane comprises the elements shown in [Figure 24 on page 582](#).

Figure 24: Main Pane Elements

The screenshot shows the 'Configure' window for 'SNMP'. The 'Traps' section is active. It features a 'Trap Group Name' input field with a red asterisk indicating it is required. Below this is a 'Categories' section with a list of checkboxes: Authentication, Chassis, Configuration, Link, Remote operations, RMON alarm, Routing, Startup, and VRRP events. A 'Targets' section contains a list box and an 'Add' button. A help tooltip is displayed over a question mark icon, providing information about the 'Targets' field: 'Targets: The value should be: A host name or IP Address'. At the bottom of the window are 'OK' and 'Cancel' buttons.

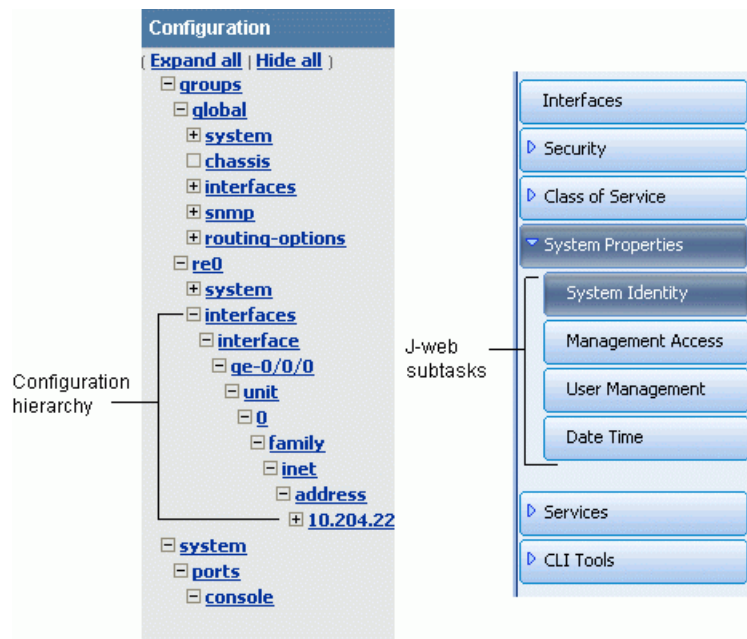
- Help (?) icon—Displays useful information when you move the cursor over the question mark. This help displays field-specific information, such as the definition, format, and valid range of the field.
- Red asterisk (\*)—Indicates a required field.
- Icon Legend— For the Edit Configuration subtask (J-Web 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 routing platform.
  - 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 25 on page 583](#).



Figure 25: 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 routing platform 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 584](#).

## 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 routing platform. 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 595](#).

After typing or selecting your configuration edits, click a button in the main pane (described in [Table 56 on page 584](#)) to move to the previous page after applying or committing the configuration. An updated configuration does not take effect until you commit it.

**Table 56: 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 routing platform. For more details, see <a href="#">“Committing a Configuration” on page 607</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 26 on page 585](#) 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 26: CoS Help Page



## Installation and Setup

- [J-Web Software Requirements on page 585](#)
- [Installing the J-Web Software on page 585](#)
- [Starting the J-Web Interface on page 586](#)
- [Configuring Basic Settings on page 588](#)

### 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 routing platform comes with the Junos OS installed on it. When you power on the routing platform, all software starts automatically. On J Series routers, the J-Web software is part of the Junos OS available by default. However, on M Series and T Series routers, you need to install the J-Web software because it is not shipped on the routing platform.

If your routing platform 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 routing platform. After the installation, you must enable Web management of the routing platform 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 routing platform.
4. Copy the software package to the routing platform. We recommend that you copy it to the `/var/tmp` directory.
5. If you have previously installed the J-Web software on the routing platform, 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 routing platform. 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 routing platform. 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 routing platform configuration described in the routing platform 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 routing platform and enabled HTTPS.



**NOTE:** If the routing platform 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 routing platform.

2. After **http://** or **https://** in your Web browser, type the hostname or IP address of the routing platform, 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 Basic Settings

Before you begin initial configuration, complete the following tasks:

- Install the routing platform in its permanent location, as described in the hardware installation guide or the Getting Started Guide for your routing platform.
- 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 27 on page 589](#)), as described in [Table 57 on page 589](#).
2. Click **Apply** to apply the configuration.

Figure 27: J-Web Set Up Initial Configuration Page

Initial Configuration

Set Up

Identification

Host Name

carol

?

Domain Name

lab.example.net

?

Root Password

••••••••

?

Verify Root Password

••••••••

?

Time

Time Zone

America/Los\_Angeles

?

NTP Servers

?

Add

Delete

Current System Time

01/20/2009 06:18

?

Set time now via NTP

?

Set time now manually

?

Network

DNS Name Servers

10.209.194.131

10.209.194.133

172.17.28.101

?

Add

Delete

Domain Search

spglab.juniper.net

apglab.juniper.net

lab.example.net

?

Add

Delete

Default Gateway

123.0.1.2

Loopback Address

192.168.8.1/32

?

fe-0/0/0.0 Address

192.168.69.205/21

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.

Apply



**NOTE:** For J Series routers only, after initial configuration is complete, the routing platform stops functioning as a Dynamic Host Configuration Protocol (DHCP) server. 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 routing platform through the J-Web interface. 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 routing platform another way—for example, through the console port.

Table 57: Initial Configuration Set Up Summary

Field	Function	Your Action
Identification		
Host Name (required)	Defines the hostname of the router.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password (required)	Sets the root password that the user “root” can use to log in to the router.	Type a plain-text password that the system encrypts.  <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.

Table 57: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
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.	<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>
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> </ul> <p><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>.</p> <ul style="list-style-type: none"> <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 127.0.0.1/32.	Type a 32-bit IP address and prefix length, in dotted decimal notation.



Table 57: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
<b>fe-0/0/0</b> Address (on J2300, J4300, and J6300 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.	Type a 32-bit IP address and prefix length, in dotted decimal notation.
<b>ge-0/0/0</b> Address (on J4350 and J6350 routers)		<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> .
<b>fxp0</b> Address (on M Series routers)		
<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.
Allow SSH Access	Allows remote access to the router by using SSH.	To enable SSH access, select the check box.

## Secure Web Access

- [Secure Web Access Overview on page 591](#)
- [Generating SSL Certificates on page 592](#)

### Secure Web Access Overview

A routing platform uses the Secure Sockets Layer (SSL) protocol to provide secure management of routing platforms 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 routing platform 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 routing platform 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 routing platform through HTTPS.

Without SSL encryption, communication between your routing platform and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

On J Series routers, 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.

## Generating SSL Certificates

To enable secure Web access, you must first generate a digital SSL certificate, and then enable HTTPS access on the routing platform.

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 612](#) to install the SSL certificate and enable HTTPS.

## CHAPTER 13

# Configuration

- [Configuration Tools on page 593](#)
- [Configuration Tasks on page 603](#)

### Configuration Tools

---

- [Configuration Task Overview on page 593](#)
- [Point and Click CLI \(J-Web Configuration Editor\) on page 595](#)
- [CLI Viewer \(View Configuration Text\) on page 597](#)
- [CLI Editor \(Edit Configuration Text\) on page 599](#)
- [CLI Terminal Requirements on page 600](#)
- [Starting the CLI Terminal on page 600](#)
- [Using the CLI Terminal on page 601](#)

### Configuration Task Overview

The J-Web user interface provides different methods for configuring your routing platform 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 routing platform, including system settings, routing protocols, interfaces, network management, and user access.

Alternatively, you can configure the routing platform services with the Junos OS command-line interface (CLI) from a console connection to the routing platform 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 601](#). 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 routing platform 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 routing platform 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 594](#).

**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 routing platform 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 routing platform.
<b>configuration hierarchy</b>	Set of hierarchically organized configuration statements that make up the Junos <sup>®</sup> OS configuration on a routing platform. 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>rescue configuration</b>	On J Series routers only, a configuration that recovers a routing platform from a configuration that denies management access. You set a current committed configuration through the J-Web interface or CLI for emergency use. To load and commit the rescue configuration, you press and release the <b>CONFIG</b> or <b>RESET CONFIG</b> button.
<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 routing platform.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the routing platform 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**. This page allows you to configure all routing platform 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 595 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.
<b>Chassis</b>	Configure routing platform chassis properties. On the Chassis pages, you can configure different properties of the routing platform chassis, including conditions that activate the red and yellow alarm LEDs on the routing platforms and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs).

Table 59: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
<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 Library 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>Junos OS Configuration and Operations Automation Library</i> .
<b>Firewall</b>	Configure stateless firewall filters. With stateless firewall filters—also known as ACLs—you can control packets transiting the routing platform to a network destination and packets destined for and sent by the routing platform. 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 routing platform, 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>Junos OS Interfaces Library 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> .
<b>Routing instances</b>	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> .

Table 59: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
<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 routing platform for use by BGP.</li> <li>• Set the router ID, which is used by BGP and OSPF to identify the routing platform 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>Junos OS VPN Library 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 28 on page 598](#)). The displayed configuration is the same as the configuration displayed when you enter the Junos OS CLI command **show configuration**.

**Figure 28: 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 routing platform. The top of the configuration displays a timestamp indicating when the configuration was last changed and the current version.

[Figure 28 on page 598](#) shows that the user committed the last configuration on 11 January 2010, and the software version running on the routing platform 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 routing platform.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the routing platform 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 29 on page 599](#)).

**Figure 29: 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 597](#).



**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 routing platform 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 routing platform, 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 588.
- 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 600.
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 routing platform.
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 30 on page 601](#)).

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 routing platform. 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 routing platform 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 30: 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 routing platform. 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 routing platform 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 routing platform.

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 routing platform 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 routing platform, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the routing platform.

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 31 on page 603 shows the CLI terminal displaying all the options that you can configure in CLI configuration mode.

Figure 31: 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# █

```

## Configuration Tasks

- [Editing and Committing a Junos OS Configuration on page 603](#)
- [J-Web Configuration Tasks on page 604](#)
- [Editing a Configuration on page 604](#)
- [Committing a Configuration on page 607](#)
- [Discarding Parts of a Candidate Configuration on page 607](#)
- [Accounting Options on page 608](#)

### 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 routing platform 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 routing platform 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 routing platform. Configuration pages provide access to all the configuration statements supported by the routing platform, 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 60 on page 604](#) provides a summary of the J-Web configuration tasks.

**Table 60: 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.	<a href="#">“Point and Click CLI (J-Web Configuration Editor)” on page 595</a>
Edit the configuration in text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	<a href="#">“CLI Editor (Edit Configuration Text)” on page 599</a>
Upload a configuration file	Upload a complete configuration.	<a href="#">“Upload Configuration File” on page 647</a>
View the configuration in text format	View the entire configuration on the routing platform in text format.	<a href="#">“CLI Viewer (View Configuration Text)” on page 597</a>

## 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 32 on page 605](#)).

Figure 32: Edit Configuration Page

**Configuration**

Expand all | Hide all |

- groups
- system

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**

- Comment**  
The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
- Inactive**  
The configuration statement is not active and does not affect the device.
- 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 61 on page 606](#) 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 61: 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 62 on page 606](#) describes the meaning of these icons.

Table 62: 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.
<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 63 on page 607](#)) 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 63: 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 routing platform. For details, see <a href="#">“Committing a Configuration” on page 607</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 607</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 routing platform.

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 644](#). 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 routing platform until you commit it.

## Accounting Options

[Figure 33 on page 609](#) 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 33: 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 14

# Administration

- [Session and User Management on page 611](#)
- [Secure Web Access on page 612](#)
- [Alarms on page 615](#)
- [Events on page 617](#)
- [Device Management on page 623](#)
- [Monitoring in J-Web on page 627](#)
- [Configuration and File Management on page 642](#)

### Session and User Management

---

- [Setting J-Web Session Limits on page 611](#)
- [Terminating J-Web Sessions on page 612](#)
- [Viewing Current Users on page 612](#)

#### Setting J-Web Session Limits

By default, an unlimited number of users can log in to the J-Web interface on a routing platform, 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 routing platform 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 routing platform 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 611](#).

## Viewing Current Users

To view a list of users logged in to the routing platform, 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 routing platform from either J-Web or the CLI.

## Secure Web Access

---

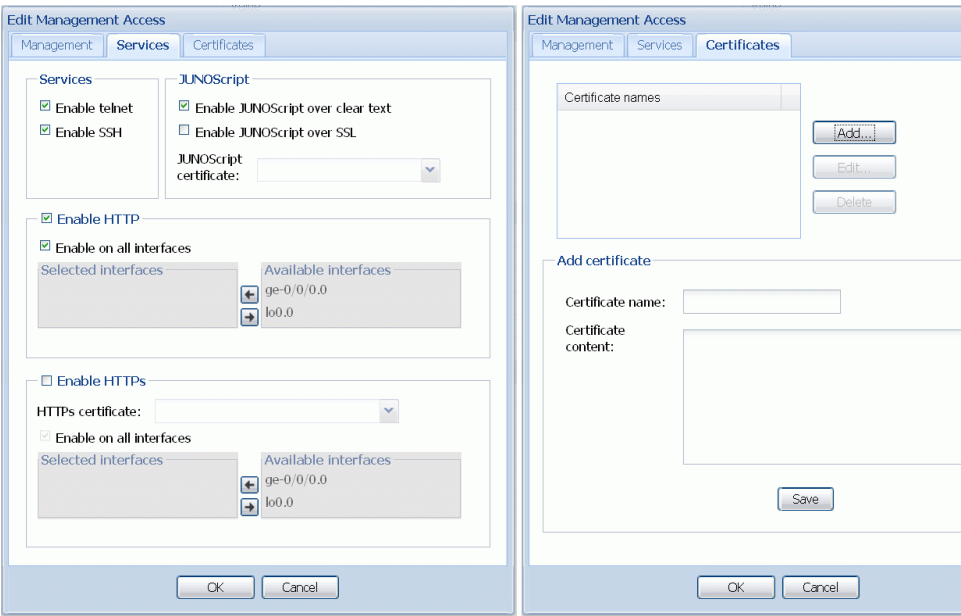
- [Configuring Secure Web Access on page 612](#)

## 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 34 on page 613](#) shows the Edit Management Access page.

Figure 34: Edit Management Access Page



To configure Web access settings in the J-Web interface:

1. Enter information into the Edit Management Access page, as described in [Table 64 on page 613](#).
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 64: Secure Access Configuration Summary

Field	Function	Your Action
Adding Certificates		
Certificate names	Displays digital certificates required for SSL access to the routing platform.  Allows you to add and delete SSL certificates.  For information about how to generate an SSL certificate, see <a href="#">“Generating SSL Certificates” on page 592</a> .	To add a certificate:  <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>

Table 64: Secure Access Configuration Summary (*continued*)

Field	Function	Your Action
To delete a certificate, select it from the list and click <b>Delete</b> .		
<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.
HTTPS certificate	<p>Specifies SSL certificates to be used for encryption.</p> <p>This field is available only after you have created an SSL certificate.</p>	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.	<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 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	<p>Specifies SSL certificates to be used for encryption.</p> <p>This field is available only after you create at least one SSL certificate.</p>	To enable an SSL certificate, select a certificate from the JUNOScript certificate list on the Services tab—for example, <b>new</b> .



---

## Alarms

---

- [Using Alarms on page 615](#)
- [View Alarms on page 615](#)
- [Active Alarms Information on page 616](#)
- [Alarm Severity on page 616](#)
- [Displaying Alarm Descriptions on page 616](#)
- [Sample Task—Viewing and Filtering Alarms on page 616](#)

### Using Alarms

You can monitor active alarms on the J-Web interface. The View Alarms page alerts you about conditions that might prevent the routing platform 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 routing platforms. An alarm indicates that you are running the routing platform 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 601](#). For more information about the commands, see [CLI Explorer](#).

### View Alarms

On J Series routers only, you can monitor active alarms on the J-Web interface. To view the alarms page, click **Monitor > Events and Alarms > Alarms**. The View Alarms page alerts you about conditions that might prevent the routing platform 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 routing platform 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 616](#)). 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 routing platform 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 routing platform 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 routing platform 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 616](#)). 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 35 on page 617](#) 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 35: 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

## Events

- [Using View Events on page 617](#)
- [Viewing Events on page 618](#)
- [View Events on page 618](#)
- [Understanding Severity Levels on page 619](#)
- [Using Filters on page 619](#)
- [Using Regular Expressions on page 621](#)
- [Sample Task—Filtering and Viewing Events on page 622](#)

## 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 routing platform.

[Figure 36 on page 618](#) 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 601](#).

```
user@host> help syslog ?
```

**Figure 36: 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
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 httpd 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 routing platform. 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 routing platform 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 routing platform, 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 routing platform. 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 routing platform power-off due to excessive temperature

On the View Events page, you can also use filters to display relevant events. [Table 66 on page 620](#) 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 routing platform functions.

[Table 65 on page 619](#) lists the system log severity levels, the corresponding colors, and a description of what the severity level indicates.

**Table 65: Severity Levels**

Color	Severity Level (from Highest to Lowest Severity)	Description
Red	<b>emergency</b>	System panic or other conditions that cause the routing platform 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 66 on page 620](#) 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 66: 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 621</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 66: 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 67 on page 621 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 67: 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 67: 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 37 on page 623 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 37: 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_SUCCESS	Authenticated httpd client (username root)	2009-07-17 04:09:54 PDT

## Device Management

- [Using Software \(J Series Routing Platforms Only\) on page 623](#)
- [Using Licenses \(J Series Routing Platform Only\) on page 624](#)
- [Using Snapshot \(J Series Routing Platforms Only\) on page 625](#)
- [Sample Task—Manage Snapshots on page 626](#)
- [Using Reboot on page 627](#)

### Using Software (J Series Routing Platforms Only)

On J Series routers only, you can upgrade and manage Junos OS packages from the J-Web interface. A Junos OS package is a collection of files that make up the software components of the routing platform.

Typically, you upgrade the Junos OS on a routing platform by downloading a set of images onto your routing platform or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the Maintain>Software page. Finally, you boot your system with this upgraded device.

As new features and software fixes become available, you must upgrade your software to use them. Before an upgrade, we recommend that you back up your primary boot device in case it becomes corrupted or fails during the upgrade. Creating a backup also stores your active configuration files and log files and ensures that you recover to a known, stable environment in case of an unsuccessful upgrade. For more information about creating a system backup, see [“Sample Task—Manage Snapshots” on page 626](#).

During a successful upgrade, the upgrade package completely reinstalls the existing software. The upgrade process rebuilds the file system but retains configuration files, log files, and similar information from the previous version.

[Table 68 on page 624](#) lists the different tasks that you can perform from the Maintain>Software pages.

Table 68: Manage Software Tasks Summary

Manage Software Task	Function
<b>Upload Package</b>	<p>Install software packages uploaded from your computer to the routing platform.</p> <ul style="list-style-type: none"> <li>File to Upload (required)—Specifies the location of the software package. Type the location of the software package, or click <b>Browse</b> to navigate to the location.</li> <li>Reboot If Required—If this check box is selected, the router is automatically rebooted when the upgrade is complete. Select the check box if you want the router to reboot automatically when the upgrade is complete.</li> </ul> <p>Click <b>Upload Package</b> to begin, and click <b>Cancel</b> to clear the entries and return to the previous page.</p>
<b>Install Package</b>	<p>Install software packages on the routing platform that are retrieved with FTP or HTTP from the location specified.</p> <ul style="list-style-type: none"> <li>Package Location—Specifies the FTP or HTTP server, file path, and software package name. The software is activated after the router has rebooted.</li> <li>User—Specifies the username, if the server requires one.</li> <li>Password—Specifies the password, if the server requires one.</li> <li>Reboot If Required—If this check box is selected, the router is automatically rebooted when the upgrade is complete.</li> </ul> <p>Click <b>Fetch and Install Package</b> to begin.</p>
<b>Downgrade</b>	<p>Downgrade the Junos OS on the routing platform.</p> <p>When you downgrade the software to a previous version, the software version that is saved in <b>junos.old</b> is the version of Junos OS that your router is downgraded to. For your changes to take effect, you must reboot the router.</p> <p><b>CAUTION:</b> After you perform this operation, you cannot undo it.</p>

Alternatively, you can install software packages on your routing platform by entering the **request system software add** command at the J-Web CLI terminal.

### Using Licenses (J Series Routing Platform Only)

The Maintain>Licenses page displays a summary of the licenses needed and used for each feature that requires a license on a J Series routing platform. This page also allows you to add licenses.

To enable some Junos OS features on a J Series routing platform, you must purchase, install, and manage separate software licenses. The presence on the router of the appropriate software license keys (passwords) determines the features you can configure and use. Each feature license is tied to exactly one software feature, and that license is valid for exactly one J Series routing platform.

Using the Maintain>Licenses page, you can perform the following tasks:

- Add licenses—Add license keys for the following features:
  - Flow monitoring traffic analysis support

- Advanced Border Gateway Protocol (BGP) features that enable route reflectors for readvertising BGP routes to internal peers.
- Delete licenses—Delete one or more license keys from a J Series routing platform with the J-Web license manager.
- Display license keys—Display the license keys in text format. Multiple licenses are separated by a blank line.

Alternatively, you can run the following commands at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 601](#). For more information about the commands, see [CLI Explorer](#).

- **show system license**—Display license information.
- **request system license add**—Add licenses on J Series routers.

For more information about licenses, see the Getting Started Guide for your J Series router.

### Using Snapshot (J Series Routing Platforms Only)

The Maintain>Snapshot page allows you to configure storage devices to replace the primary boot device on your router or to act as a backup boot device. To do so, you create a snapshot of the system software running on your router, saving the snapshot to an alternative storage device.

The Manage Snapshot page allows you to perform the following tasks:

- Copy the current system software, along with the current and rescue configurations, to an alternative storage device.



**CAUTION:** We recommend that you keep your secondary storage medium updated at all times. If the internal compact flash fails at startup, the J Series routing platform automatically boots itself from this secondary storage medium. The secondary storage medium can be either an external compact flash or a USB storage device. When a secondary storage medium is not available, the routing platform is unable to boot and does not come back online. This situation can occur if the power fails during a Junos OS upgrade and the physical or logical storage media on the routing platform are corrupted. The backup device must have a storage capacity of at least 256 MB.

- Copy only default files that were loaded on the internal compact flash when it was shipped from the factory, plus the rescue configuration, if one has been set.
- Configure a boot device to store snapshots of software failures, for use in troubleshooting.
- Partition the storage medium. This process is usually necessary for storage devices that do not already have software installed on them.

- Create a snapshot for use as the primary boot device to replace the device in the internal compact flash slot or to replicate it for use in another J Series routing platform. You can perform this action only on a removable storage device.
- Specify the size of the following partitions in kilobytes:
  - **data**—Data partition is not used by the routing platform, and can be used for extra storage.
  - **swap**—Swap partition is used for swap files and software failure memory snapshots. Software failure memory snapshots are saved to the boot medium only if it is specified as the dump device.
  - **config**—Config partition is used for storing configuration files.
  - **root**—Root partition does not include configuration files.

Click **Snapshot** to begin.

Alternatively, you can use the **request system snapshot** command in the J-Web CLI terminal to take a snapshot of the routing platform. For information about installing boot devices, see the Getting Started Guide for your J Series router.

## Sample Task—Manage Snapshots

Figure 38 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 routing platform. A compact flash is connected to the USB port on the J Series routing platform with a USB adapter.

To take the snapshot:

1. Select **Maintain>Snapshot** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 38 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 38: 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 routing platform 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 routing platform by running the **request system reboot** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 601](#). For more information about the **request system reboot** command, see [CLI Explorer](#).

## Monitoring in J-Web

- [Monitor Task Overview on page 628](#)
- [Chassis Viewer \(M7i, M10i, M20, M120, and M320 Routing Platforms Only\) on page 628](#)
- [Class of Service on page 629](#)
- [Interfaces on page 630](#)
- [MPLS on page 631](#)

- [PPPoE \(J Series Routing Platforms Only\) on page 632](#)
- [RPM on page 632](#)
- [Routing on page 633](#)
- [Security on page 634](#)
- [Service Sets on page 636](#)
- [Services on page 636](#)
- [System View on page 636](#)
- [Sample Task—Monitoring Interfaces on page 638](#)
- [Sample Task—Monitoring Route Information on page 640](#)

## Monitor Task Overview

Use the J-Web Monitor tasks to monitor your routing platform. The J-Web interface displays diagnostic information about the routing platform in the browser.

You can also monitor the routing platform 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 601](#). 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.

## Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only)

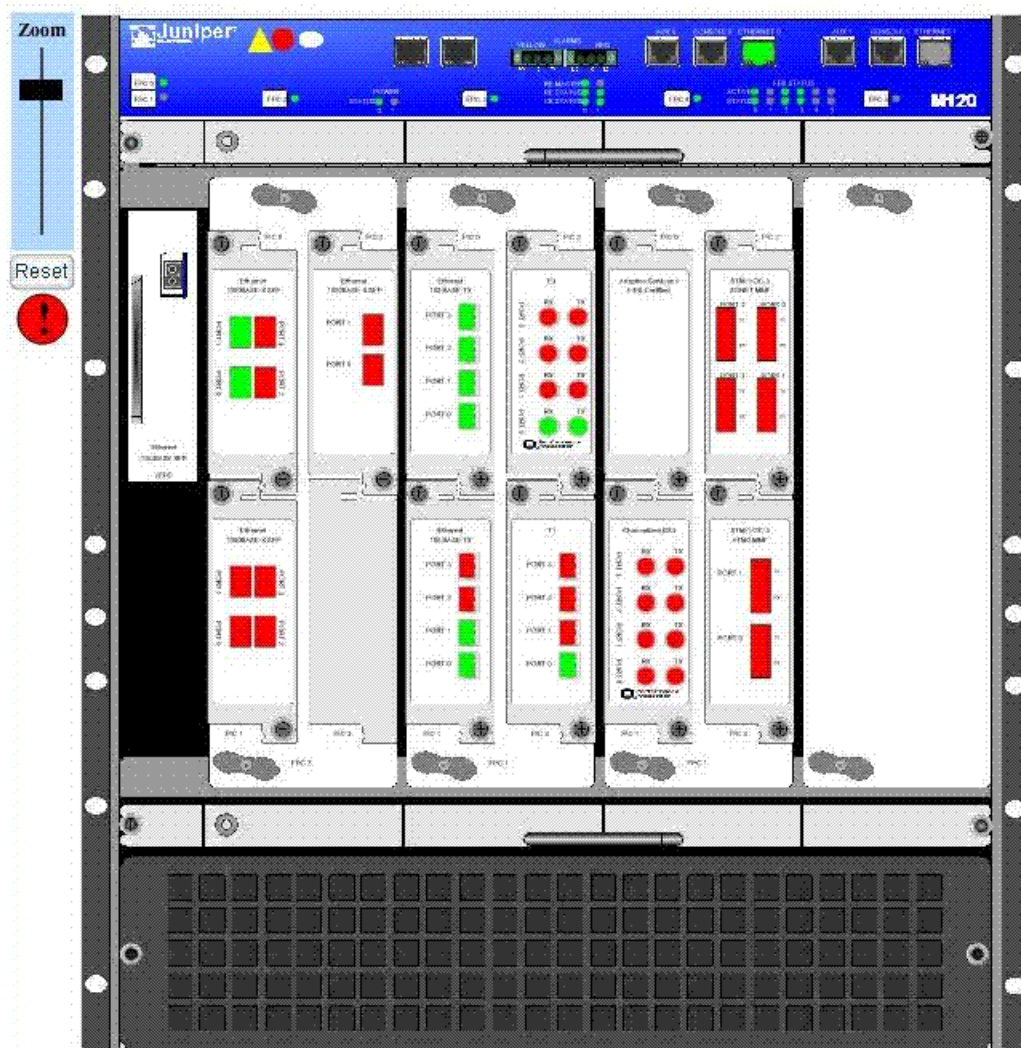
On M7i, M10i, M20, M120, and M320 routers, you can use the chassis viewer feature to view images of the chassis and access information about each component similar to what you can obtain using the **show chassis alarms** and **show chassis hardware** commands.

To access the chassis viewer, click **Chassis** in the upper-right corner of any J-Web page for an M7i, M10i, M20, M120, or M320 routing platform. A separate page appears to display the image of the chassis and its component parts, including power supplies, individual Physical Interface Cards (PICs), and ports. Major or minor alarm indicators appear in red.

[Figure 39 on page 629](#) shows the chassis and components of an M120 routing platform. It also shows the status of each port in red or green, and the zoom bar selections.

Figure 39: Chassis Viewer Page

Click and drag the chassis to pan the image. Hover over a FRU for status information(serial number, description, etc.). Right click on the chassis for more options such as configuration and monitoring. Router status lights are updated every 1 minute.



## Class of Service

To display details about the performance of class of service (CoS) on a routing platform, select **Monitor > Class of Service** in the J-Web interface.

Table 69 on page 630 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 69: 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 routing platform 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 638.)

[Table 70 on page 631](#) 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 70: 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 routing platform.	<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 71 on page 631](#) 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 71: 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 routing platform, 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 routing platform, 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 routing platform, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	<b>show rsvp session</b>
<b>RSVP Interfaces</b>	
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>

## PPPoE (J Series Routing Platforms Only)

The Point-to-Point Protocol over Ethernet (PPPoE) monitoring information is displayed in multiple parts. To display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the routing platform, and the PPPoE version configured on the routing platform, select **Monitor>PPPoE** in the J-Web interface.

To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

[Table 72 on page 632](#) shows a summary of the information displayed on the PPPoE page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

**Table 72: PPPoE Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Session-specific information about the interfaces on which PPPoE is enabled.	<b>show pppoe interfaces</b>
Statistics for PPPoE sessions currently active.	<b>show pppoe statistics</b>
PPPoE protocol currently configured on the routing platform.	<b>show pppoe version</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 routing platform. To view these RPM properties, select **Troubleshoot > RPM** in the J-Web interface.

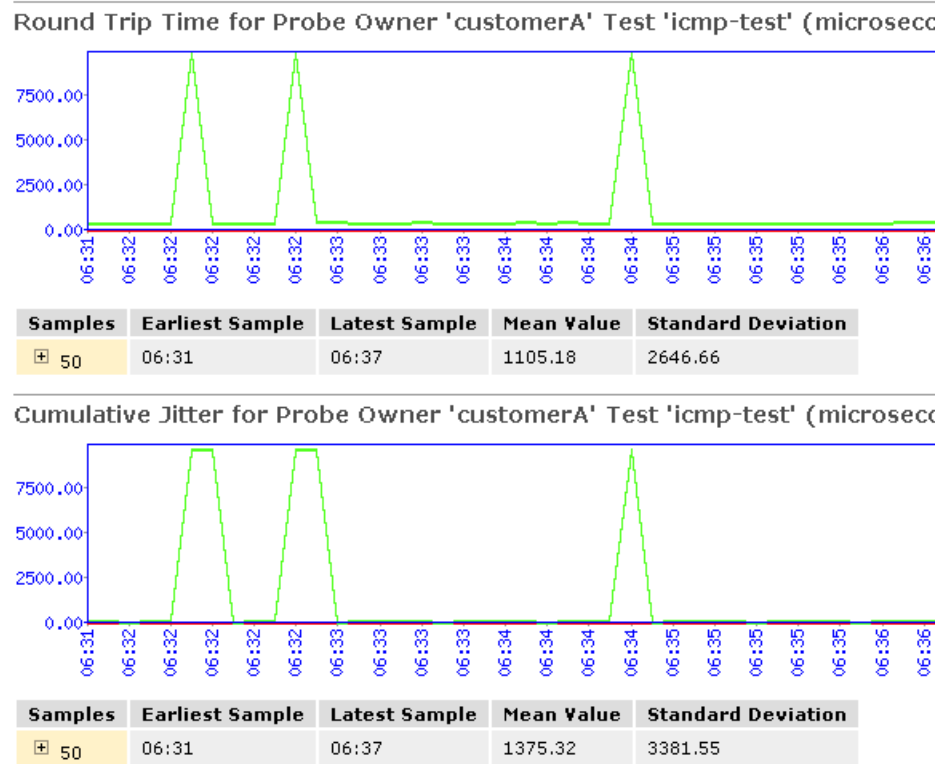
[Table 73 on page 632](#) shows a summary of the information displayed on the RPM page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

**Table 73: 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 40 on page 633](#) shows sample graphs for an RPM test.

Figure 40: Sample RPM Graphs



In [Figure 40 on page 633](#), 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 74 on page 633](#) 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 74: 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 74: 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 634](#)
- [IPsec on page 635](#)
- [NAT on page 635](#)

### 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 75 on page 634](#) 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 75: 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>

**Table 75: Firewall Information and the Corresponding CLI show Commands** (*continued*)

Information Displayed	Corresponding CLI Command
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 76 on page 635](#) 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 76: 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 routing platform. To view NAT pool information, select **Monitor>Security>NAT** in the J-Web interface.

[Table 77 on page 635](#) 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 77: 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 routing platform, 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 78 on page 636](#) 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 78: 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

A J Series routing platform can operate as a Dynamic Host Configuration Protocol (DHCP) server. To view information about dynamic and static DHCP leases, conflicts, pools, and statistics, select **Monitor>Services>DHCP** in the J-Web interface.

[Table 79 on page 636](#) 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 79: 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 637](#)
- [Chassis Information on page 637](#)
- [Process Details on page 637](#)
- [FEB Redundancy \(M120 Routing Platforms Only\) on page 638](#)

### System Information

To view information about system properties such as the name and IP address of the routing platform or the resource usage on the Routing Engine, select **Monitor>System View** in the J-Web interface.

Table 80 on page 637 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 80: System Information and the Corresponding CLI show Commands**

Information Displayed	Corresponding CLI Command
Current time and information about how long the routing platform, routing platform software, and routing protocols have been running.	<b>show system uptime</b>
Information about users who are currently logged in to the routing platform.	<b>show system users</b>
Statistics about the amount of free disk space in the routing platform's file systems.	<b>show system storage</b>
Software processes running on the routing platform.	<b>show system processes</b>

### Chassis Information

To view chassis properties on the routing platform, select **Monitor>System View>Chassis Information** in the J-Web interface.

Table 81 on page 637 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 81: 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 routing platform 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>
List of all FPCs and PICs installed in the routing platform 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 82 on page 638](#) 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 82: 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 83 on page 638](#) 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 83: FEB Redundancy Information and the Corresponding CLI show Command**

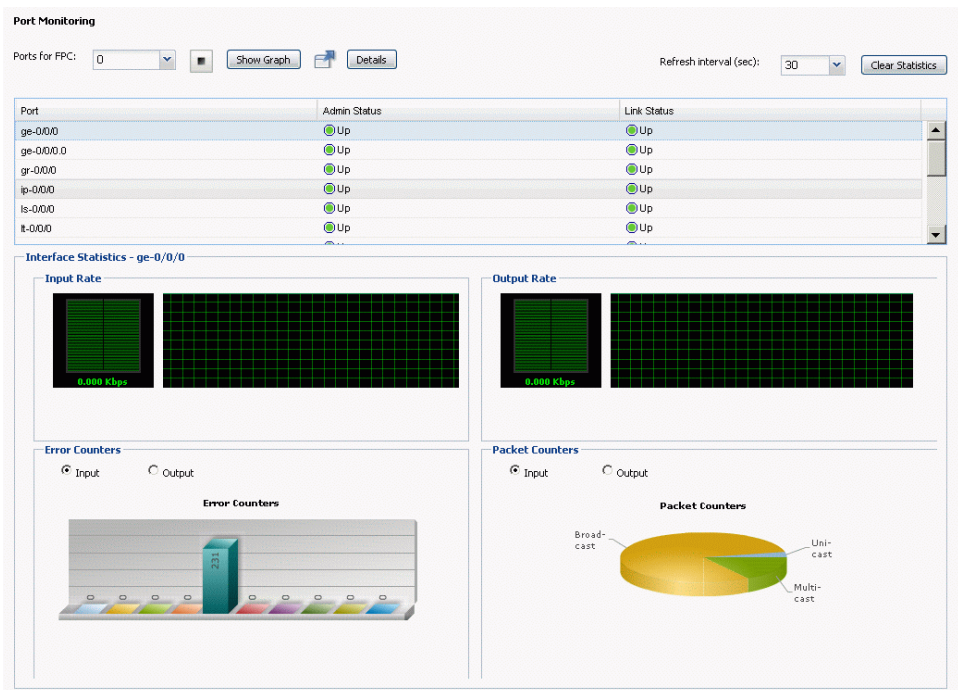
Information Displayed	Corresponding CLI Command
Forwarding Engine Board (FEB) status information.	<b>show chassis feb</b>

### **Sample Task—Monitoring Interfaces**

[Figure 41 on page 639](#) shows the Port Monitoring page that displays the interfaces installed on your routing platform. At a glance, you can monitor the status of all the configured physical and logical interfaces.



Figure 41: 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 42 on page 640](#)).

Figure 42: 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 43 on page 641 shows the Route Information monitoring page that displays information about all 9 routes in the routing table. All routing platforms are active, and there are no hidden routes.

Figure 43: 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 44 on page 641](#)).

Figure 44: 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

## Configuration and File Management

---

- [Displaying Configuration History on page 642](#)
- [Displaying Users Editing the Configuration on page 644](#)
- [Loading a Previous Configuration File on page 645](#)
- [Downloading a Configuration File on page 646](#)
- [Comparing Configuration Files on page 646](#)
- [Upload Configuration File on page 647](#)
- [Using Rescue \(J Series Routing Platforms Only\) on page 648](#)
- [Using Files on page 648](#)

### Displaying Configuration History

When you commit a configuration, the routing platform 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 45 on page 643](#)).

[Table 84 on page 643](#) 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 routing platform.

Figure 45: 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".

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 84: 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 84: 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 599</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 647</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 645</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 646</a> and <a href="#">“Loading a Previous Configuration File” on page 645</a> .

For more information about saved versions of configuration files, see [“Editing and Committing a Junos OS Configuration” on page 603](#).

## Displaying Users Editing the Configuration

To display a list of users editing the routing platform configuration, select **Maintain>Config Management>History**. The list is displayed as Database Information in the main pane (see [Figure 46 on page 645](#)). [Table 85 on page 645](#) summarizes the Database Information display.

Figure 46: 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 85: 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 routing platform.
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 routing platform.
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 routing platform:

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 routing platform 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 routing platform 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 47 on page 647](#)):

- 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 47: J-Web Configuration File Comparison Results

History

Compare Rollback 5 Configuration to Rollback 2 Configuration

Legend:

Removed from Rollback 5 Configuration

changed lines

Added in Rollback 2 Configuration

Rollback 5 Configuration	Rollback 2 Configuration
<div>[edit]</div> <div>version 9.1B2.8;</div>	<div>[edit]</div> <div>version "9.410 [builder]";</div> <div>system {</div> <div>  domain-name englab.juniper.net;</div> <div>  domain-search [ englab.juniper.net juniper.net jnpr.net spglab.juniper.net ];</div> <div>  backup-router 10.209.63.254;</div> <div>  services {</div> <div>    rlogin;</div> <div>    rsh;</div> <div>    ssh;</div> <div>    telnet;</div> <div>    web-management {</div> <div>      http;</div> <div>    }</div> <div>  }</div> <div>  routing-options {</div> <div>    static {</div> <div>      route 0.0.0.0/0 next-hop 10.209.63.254;</div> <div>    }</div> <div>  }</div> <div>}</div>

Legend:

Removed from Rollback 5 Configuration

changed lines

Added in Rollback 2 Configuration

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 48 on page 648).
  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 routing platform checks the configuration for the correct syntax before committing it.

Figure 48: J-Web Upload Configuration File Page

**Config Management**

**Upload**

Type the name of a configuration file on the local hard drive. When you click "Upload and Commit", the configuration in the file replaces the existing configuration and takes effect. If any errors occur when the file is loaded, configuration is restored.

• File to Upload   ?

## Using Rescue (J Series Routing Platforms Only)

If someone inadvertently commits a configuration that denies management access to a routing platform, you can delete the invalid configuration and replace it with a rescue configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI. The rescue configuration is a previously committed, valid configuration.

To view, set, or delete the rescue configuration, select **Maintain>Rescue**. On the Rescue page (see [Figure 49 on page 648](#)), you can perform the following tasks:

- View the current rescue configuration (if one exists)—Click **View rescue configuration**.
- Set the current running configuration as the rescue configuration—Click **Set rescue configuration**. On a J Series routing platform, you can also press the **CONFIG** or **RESET CONFIG** button.
- Delete the current rescue configuration—Click **Delete rescue configuration**.

Figure 49: Rescue Configuration Page

**Rescue**

If you inadvertently commit a configuration that denies management access, the only recourse may be to connect the console. The rescue configuration gives you another alternative. The rescue configuration is a configuration you know will allow management access to the router.

Press and immediately release the Config button on the chassis to cause the router to load and commit the rescue configuration. This will put the router back into a manageable state. You must have set the rescue configuration for this feature to function properly.

**View Rescue Configuration**

The rescue configuration for the router has been set. To view the rescue configuration, click the link below.

[View rescue configuration](#)

**Set or Delete Rescue Configuration**

Clicking 'Set rescue configuration' will set the rescue configuration to the current running configuration of the router. Clicking 'Delete rescue configuration' will delete the rescue configuration.

[Set rescue configuration](#)

[Delete rescue configuration](#)

## Using Files

Select **Maintain>Files** in the J-Web interface to manage log, temporary, and core files on the routing platform.

[Table 86 on page 649](#) lists the different tasks that you can perform from the **Maintain > Files** page.

**Table 86: Manage Files Tasks Summary**

Manage Files Task	Functions
<b>Clean Up Files</b>	<p>Rotate log files and delete unnecessary files on the routing platform. 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 601</a>. For more information about the <b>request system storage cleanup</b> command, see <a href="#">CLI Explorer</a>.</p>
<b>Download and Delete Files</b>	<p>Download a copy of an individual file or delete it from the routing platform. 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 <b>/cf/var/log</b> directory on the router.</li> <li><b>Temporary Files</b>—Lists the temporary files located in the <b>/cf/var/tmp</b> directory on the router.</li> <li><b>Old Junos OS</b>—Lists the existing Junos OS packages in the <b>/cf/var/sw</b> directory on the router.</li> <li><b>Crash (Core) Files</b>—Lists the core files located in the <b>/cf/var/crash</b> 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 routing platform. 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>



## CHAPTER 15

# Troubleshooting

- [J-Web User Interface on page 651](#)
- [Events on page 652](#)
- [Network on page 653](#)

### 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 routing platform through J-Web.
- Cause**      For J Series routers only, after initial configuration is complete, the routing platform stops functioning as a Dynamic Host Configuration Protocol (DHCP) server. 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 routing platform 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 routing platform 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 routing platform 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 585](#).

**Solution 2**—If the routing platform 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 routing platform.

## 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 is the 'Events Detail' section, which contains a table with columns: Process, Severity, Event ID, Event Description, and Time. The table is currently empty, displaying the message 'No events match filter condition'. A 'Generate Report' button is located to the right of the table.

**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#

```

## Network

- [Using Ping Host on page 653](#)
- [Using Ping MPLS on page 654](#)
- [Using Ping ATM \(M Series, MX Series, and T Series Routing Platforms Only\) on page 656](#)
- [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 routing

platform 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 routing platform 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 601](#). 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 routing platform 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 87 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 601](#).



Table 87: 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>Junos OS Interfaces Library 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 87: 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 Ping ATM (M Series, MX Series, and T Series Routing Platforms Only)

On M Series, MX Series, and T Series routers, use the Ping ATM pages to ping an Asynchronous Transfer Mode (ATM) node on an ATM virtual circuit (VC) pathway to verify that the node can be reached over the network. The output is useful for diagnosing ATM node and network connectivity problems. The routing platform sends a series of echo requests to a specified ATM node and receives echo responses.

Alternatively, you can enter the `ping atm` command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 601](#). For more information about the `ping atm` command, see [CLI Explorer](#).

### Using Traceroute

Use the Traceroute page to trace a route between the routing platform and a remote host. You can use the traceroute task to display a list of routers between the routing platform and a specified destination host. The output is useful for diagnosing a point of failure in the path from the routing platform to the destination host, and addressing network traffic latency and throughput problems.

The routing platform 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 routing platform 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 routing platform 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 601](#). 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 routing platform. 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 601](#). 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. For details, see the *J-series Services Router Administration Guide*.

## Sample Task—Ping Host

[Figure 52 on page 658](#) 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 658](#)).
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 routing platform 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**

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 ☐ ?

Interface  ?

Count  ?

Don't Fragment ☐ ?

Record Route ☐ ?

Type-of-Service  ?

Routing Instance  ?

Interval  ?

Packet Size  ?

Source Address  ?

Time-to-Live  ?

Bypass Routing ☐ ?

Figure 53 on page 658 displays the results of a successful ping in the main pane, and Table 88 on page 658 provides a summary of the ping host results and output.

Figure 53: Successful Ping Host Results Page

**Ping Host**

**Ping 10.10.2.2**

```

PING 10.10.2.2 (10.10.2.2): 56 data bytes
64 bytes from 10.10.2.2: icmp_seq=0 ttl=58 time=259.730 ms
64 bytes from 10.10.2.2: icmp_seq=1 ttl=58 time=259.555 ms
64 bytes from 10.10.2.2: icmp_seq=2 ttl=58 time=258.501 ms
64 bytes from 10.10.2.2: icmp_seq=3 ttl=58 time=258.516 ms
64 bytes from 10.10.2.2: icmp_seq=4 ttl=58 time=258.547 ms
64 bytes from 10.10.2.2: icmp_seq=5 ttl=58 time=365.037 ms
64 bytes from 10.10.2.2: icmp_seq=6 ttl=58 time=261.953 ms
64 bytes from 10.10.2.2: icmp_seq=7 ttl=58 time=257.491 ms
64 bytes from 10.10.2.2: icmp_seq=8 ttl=58 time=257.492 ms
64 bytes from 10.10.2.2: icmp_seq=9 ttl=58 time=258.303 ms
--- 10.10.2.2 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 257.491/269.512/365.037/31.865 ms

```

Table 88: 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.

Table 88: J-Web Ping Host Results and Output Summary (continued)

Ping Host Result	Description
icmp_seq=number	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 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 Library for Security Devices

- [Administration Guide for Security Devices on page 663](#)
- [Access Privilege Administration Guide on page 1059](#)





## CHAPTER 16

# Administration Guide for Security Devices

- [Overview on page 663](#)
- [Configuration on page 699](#)
- [Administration on page 888](#)

## Overview

---

- [Secure Web Access on page 663](#)
- [J-Web User Interface on page 664](#)
- [User Authentication and Access on page 671](#)
- [USB Modems for Remote Management Setup on page 676](#)
- [Telnet and SSH Device Control on page 681](#)
- [DHCP for IP Address Device on page 684](#)
- [DHCPv6 Client on page 692](#)
- [DHCPv6 Local Server on page 694](#)
- [File Management on page 695](#)
- [Licenses on page 695](#)

## Secure Web Access

- [Secure Web Access Overview on page 663](#)

### 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 888](#)
- [Generating a Self-Signed SSL Certificate on page 889](#)
- [Configuring Device Addresses on page 890](#)
- [Example: Configuring Secure Web Access on page 892](#)
- *Administration Guide for Security Devices*

## J-Web User Interface

- [Understanding the User Interfaces on page 664](#)
- [Starting the J-Web User Interface on page 666](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [J-Web Commit Options Guidelines on page 669](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- [Establishing J-Web Sessions on page 671](#)

### 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 665](#)
- [CLI on page 666](#)

### ***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 SRX100, SRX210, SRX220, SRX240, and SRX650 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.

**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*.

**Related Documentation**

- [Starting the J-Web User Interface on page 666](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- *CLI User Guide*
- *Administration Guide for Security Devices*

**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 89 on page 666](#) shows the maximum number of concurrent Web sessions on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

**Table 89: Concurrent Web Sessions on SRX Series Devices**

SRX100	SRX210	SRX220	SRX240	SRX650
3	3	3	5	5

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 664](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [J-Web Commit Options Guidelines on page 669](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- [Establishing J-Web Sessions on page 671](#)
- [Administration Guide for Security Devices](#)

### 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**—Displayd 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 664](#)
- [Starting the J-Web User Interface on page 666](#)
- [J-Web Commit Options Guidelines on page 669](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- [Establishing J-Web Sessions on page 671](#)
- *Administration Guide for Security Devices*

### 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 664](#)
- [Starting the J-Web User Interface on page 666](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- [Establishing J-Web Sessions on page 671](#)
- *Administration Guide for Security Devices*

---

### 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 664](#)
- [Starting the J-Web User Interface on page 666](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [J-Web Commit Options Guidelines on page 669](#)
- [Establishing J-Web Sessions on page 671](#)



- *Administration Guide for Security Devices*

### 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 664](#)
- [Starting the J-Web User Interface on page 666](#)
- [Understanding the J-Web Interface Layout on page 667](#)
- [J-Web Commit Options Guidelines on page 669](#)
- [Getting Help in the J-Web User Interface on page 670](#)
- *Administration Guide for Security Devices*

## User Authentication and Access

- [Understanding User Authentication Methods on page 671](#)
- [Understanding User Accounts on page 672](#)
- [Understanding Login Classes on page 673](#)
- [Understanding Template Accounts on page 676](#)

### 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 672](#)
- [Understanding Login Classes on page 673](#)
- [Understanding Template Accounts on page 676](#)
- *Administration Guide for Security Devices*

---

### Understanding User Accounts

User accounts provide one way for users to access the device. Users can access the device without accounts if you configured RADIUS or TACACS+ servers. After you have created an account, the device creates a home directory for the user. An account for the user **root** is always present in the configuration. For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username.
- User's full name—If the full name contains spaces, enclose it in quotation marks (" "). Do not include colons or commas.
- User identifier (UID)—Numeric identifier that is associated with the user account name. The identifier range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
- User's access privilege—You can create login classes with specific permission bits or use one of the predefined classes.
- Authentication method or methods and passwords that the user can use to access the device—You can use SSH or an MD5 password, or you can enter a plain-text password that Junos OS encrypts using MD5-style encryption before entering it in the password database. If you configure the plain-text-password option, you are prompted to enter and confirm the password.

**Related  
Documentation**

- [Understanding User Authentication Methods on page 671](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 895](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 897](#)
- [Example: Configuring Authentication Order on page 900](#)
- *Administration Guide for Security Devices*

### 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.

[Table 90 on page 673](#) contains a few predefined login classes. The predefined login classes cannot be modified.

**Table 90: Predefined Login Classes**

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
super-user and superuser	all
unauthorized	None

This section contains the following topics:

- [Permission Bits on page 673](#)
- [Denying or Allowing Individual Commands on page 675](#)

#### **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 91 on page 674](#)).

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 91: Permission Bits for Login Classes

Permission Bit	Access
<b>admin</b>	Can view user account information in configuration mode and with the <b>show configuration</b> command.
<b>admin-control</b>	Can view user accounts and configure them (at the <b>[edit system login]</b> hierarchy level).
<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.

Table 91: Permission Bits for Login Classes (*continued*)

Permission Bit	Access
<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 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 671](#)
- [Understanding User Accounts on page 672](#)

- [Understanding Template Accounts on page 676](#)
- [Example: Configuring New Users on page 902](#)
- *Administration Guide for Security Devices*

---

### 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 671](#)
- [Understanding User Accounts on page 672](#)
- [Understanding Login Classes on page 673](#)
- [Example: Creating Template Accounts on page 908](#)
- *Administration Guide for Security Devices*

## USB Modems for Remote Management Setup

- [USB Modem Interface Overview on page 676](#)
- [USB Modem Configuration Overview on page 679](#)

---

### 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 92 on page 678](#) describes the commands. For more information about these commands, see the documentation for your modem.

**Table 92: Default Modem Initialization Commands**

Modem Command	Description
<code>AT</code>	Attention. Informs the modem that a command follows.
<code>S7=45</code>	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
<code>S0=0</code>	Disables the auto answer feature, whereby the modem automatically answers calls.
<code>V1</code>	Displays result codes as words.
<code>&amp;C1</code>	Disables reset of the modem when it loses the carrier signal.
<code>E0</code>	Disables the display on the local terminal of commands issued to the modem from the local terminal.
<code>Q0</code>	Enables the display of result codes.
<code>&amp;Q8</code>	Enables Microcom Networking Protocol (MNP) error control mode.



Table 92: Default Modem Initialization Commands (*continued*)

Modem Command	Description
%C0	Disables data compression.

When the device applies the modem AT commands in the **init-command-string** command or the default sequence of initialization commands to the modem, it compares them to the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include **S0=0** and the device's **init-command-string** command includes **S0=2**, the device applies **S0=2**.
- If the initialization commands on the modem do not include a command in the device's **init-command-string** command, the device adds it. For example, if the **init-command-string** command includes the command **L2**, but the modem commands do not include it, the device adds **L2** to the initialization commands configured on the modem.

#### Related Documentation

- [USB Modem Configuration Overview on page 679](#)
- [Example: Configuring a USB Modem Interface on page 699](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 705](#)
- *Administration Guide for Security Devices*
- *Modem Interfaces Feature Guide for Security Devices*

#### 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:** J Series devices have two USB ports. However, you can connect only one USB modem to the USB ports on these devices. If you connect USB modems to both ports, the device detects only the first modem connected.



**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 93 on page 680](#) for a summarized description of the procedure.

**Table 93: 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"</a> on page 699.
	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"</a> on page 705.

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 94 on page 681](#) for a list of available incoming map options.

**Table 94: 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 676](#)
- [Example: Configuring a USB Modem Interface on page 699](#)
- *Administration Guide for Security Devices*
- *Modem Interfaces Feature Guide for Security Devices*

## Telnet and SSH Device Control

- [Securing the Console Port Configuration Overview on page 681](#)
- [Reverse Telnet Overview on page 683](#)

### 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 of 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 928](#)
- [The ssh Command on page 929](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Reverse Telnet Overview on page 683](#)
- [Configuring Reverse Telnet and Reverse SSH on page 924](#)
- [Administration Guide for Security Devices](#)

## Reverse Telnet Overview

Reverse telnet allows you to configure a device to listen on a specific port for Telnet and SSH services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You use a rollover cable to connect the auxiliary port from the device on which reverse telnet is enabled to the console port of the device you want to manage.



**NOTE:** Reverse telnet is supported only on J Series devices.

To use reverse telnet, you must have the following devices:

- A device with an auxiliary port running the appropriate version of Junos OS.
- A device with a console port for remote management if network connectivity fails and you want to use console access.

This section contains the following topics:

- [Reverse Telnet Options on page 683](#)
- [Reverse Telnet Restrictions on page 683](#)

### Reverse Telnet Options

When you enable reverse telnet, you can control the port that is used, and you can optionally turn on reverse ssh to encrypt the reverse telnet communication between the device and the client. By default, reverse telnet uses port 2900 and reverse ssh uses port 2901.



**NOTE:** Enabling reverse ssh requires an additional command. By default, when you enable reverse telnet, the connection is not encrypted.

### Reverse Telnet Restrictions

Keep the following restrictions in mind when you attempt to use reverse telnet or reverse ssh:

- Multiple connections to the serial port are not allowed. If there is an existing connection to the serial port, any other connections are denied.
- If the auxiliary port is enabled (through the **system services port auxiliary** configuration statement), you cannot use reverse telnet or reverse ssh because another service is already using the auxiliary port.

#### Related Documentation

- [The telnet Command on page 928](#)
- [The ssh Command on page 929](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Configuring Reverse Telnet and Reverse SSH on page 924](#)

- *Administration Guide for Security Devices*

## DHCP for IP Address Device

- [DHCP Server, Client, and Relay Agent Overview on page 684](#)
- [DHCP Configuration Overview on page 685](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Understanding DHCP Client Operation on page 687](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- [Understanding DHCP Services in a Routing Instance on page 689](#)

### 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.

#### Related Documentation

- [DHCP Configuration Overview on page 685](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Understanding DHCP Client Operation on page 687](#)

- [Understanding DHCP Relay Agent Operation on page 687](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- *Administration Guide for Security Devices*

### DHCP 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 95 on page 685](#) provides the settings and values for the sample DHCP server configuration.

**Table 95: Sample DHCP 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

**Table 95: Sample DHCP Configuration Settings (*continued*)**

Setting	Sample Value
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
Fixed address	192.168.2.50

**Related Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 684](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Understanding DHCP Client Operation on page 687](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [RFC 3397, Dynamic Host Configuration Protocol \(DHCP\) Domain Search Option](#)
- [Administration Guide for Security Devices](#)

**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 686](#)
- [Compatibility with Autoinstallation on page 687](#)

**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.

#### **Related Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 684](#)
- [Example: Configuring the Device as a DHCP Server on page 709](#)
- [Understanding DHCP Client Operation on page 687](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- *Administration Guide for Security Devices*

### **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.

#### **Related Documentation**

- [DHCP Server, Client, and Relay Agent Overview on page 684](#)
- [Example: Configuring the Device as a DHCP Client on page 714](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- *Administration Guide for Security Devices*

### **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 684](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 718](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- *Administration Guide for Security Devices*

---

### DHCP Settings and Restrictions Overview

This section contains the following topics:

- [Propagation of TCP/IP Settings for DHCP on page 688](#)
- [DHCP Conflict Detection and Resolution on page 688](#)
- [DHCP Interface Restrictions on page 689](#)

#### ***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 684](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Understanding DHCP Client Operation on page 687](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [Administration Guide for Security Devices](#)

**Understanding DHCP Services in a Routing Instance**

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.
- In Junos Release 12.1X46, autoinstallation is not compatible with jDHCPd:

```
version 12.1X46-D40.2;
system {
  /* not compatible with jDHCPd */  <<<<<<
  autoinstallation {
    usb {
      disable;
    }
  }
}
```



**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.

#### Related Documentation

- [Configuring a DHCP Local Server on page 723](#)
- [Configuring a DHCP Client on page 727](#)
- [Configuring a DHCP Relay Agent on page 729](#)
- *Administration Guide for Security Devices*

## DHCPv6 Client

- [DHCPv6 Client Overview on page 693](#)
- [Understanding DHCPv6 Client and Server Identification on page 693](#)

## 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.

### Related Documentation

- [Minimum DHCPv6 Client Configuration on page 736](#)

## 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 693](#)

### DHCPv6 Local Server

- [DHCPv6 Server Overview on page 694](#)

---

#### 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 and J 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 743](#)
- [Example: Configuring an Address-Assignment Pool on page 745](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 748](#)
- [Creating a Security Policy for DHCPv6 on page 742](#)
- *Administration Guide for Security Devices*

## File Management

- [File Management Overview on page 695](#)

### 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 934](#)
- [Cleaning Up Files with the CLI on page 935](#)
- [Managing Accounting Files on page 938](#)
- [Encrypting Configuration Files on page 932](#)
- *Network Monitoring and Troubleshooting Guide for Security Devices*
- [Junos OS System Log Reference for Security Devices](#)

## Licenses

- [Junos OS License Overview on page 696](#)
- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 698](#)

## Junos OS License Overview

---

To enable some Junos OS features, you must purchase, install, and manage separate software licenses. For those features that require a license, the presence on the device of the appropriate software license keys (passwords) determines whether you can use the feature.

For information about how to purchase software licenses for your device, contact your Juniper Networks sales representative.

Certain Junos OS features require licenses. Each license is valid for only a single device. To manage the licenses, you must understand license enforcement and the components of a license key.

This section contains the following topics:

- [License Enforcement on page 696](#)
- [License Key Components on page 696](#)
- [License Management Fields Summary on page 697](#)

### ***License Enforcement***

For features that require a license, you must install and properly configure the license to use the feature. Although the device allows you to commit a configuration that specifies a feature requiring a license when the license is not present, you are prohibited from actually using the feature.

Successful commitment of a configuration does not imply that the required licenses are installed. If a required license is not present, the system provides a warning message after it commits the configuration rather than failing to commit it because of a license violation.

### ***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 26 on page 157](#).

**Table 96: Summary of License Management Fields**

Field Name	Definition
<b>Feature Summary</b>	
Feature	Name of the licensed feature: <ul style="list-style-type: none"> <li>• <b>Features</b>—Software feature licenses.</li> <li>• <b>All features</b>—All-inclusive licenses</li> </ul>
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.
<b>Installed Licenses</b>	
ID	Unique alphanumeric ID of the license.
State	<b>Valid</b> —The installed license key is valid.  <b>Invalid</b> —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.  <b>NOTE:</b> 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

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)

- [Saving License Keys on page 255](#)
- [Downloading License Keys on page 255](#)
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

### Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways

For information about how to purchase a software license, contact your Juniper Networks sales representative at <http://www.juniper.net/in/en/contact-us/>.

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. [Table 27 on page 160](#) describes the Junos OS features that require licenses.

**Table 97: 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

Table 97: Junos OS Feature Licenses (*continued*)

Junos OS License Requirements										
Feature	SRX100	SRX110	SRX210	SRX220	SRX240	SRX550	SRX650	SRX1400	SRX3000 line	SRX5000 line
SRX100 Memory Upgrade	X									
UTM	X*	X	X *	X	X *	X	X	X	X	X

\* Indicates support on high-memory devices only.

Each license allows you to run the specified advanced software features on a single device.

#### Related Documentation

- [Junos OS License Overview on page 156](#)
- *Installation and Upgrade Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

## Configuration

- [USB Modems for Remote Management Setup on page 699](#)
- [DHCP for IP Address Device on page 708](#)
- [DHCPv6 Client on page 736](#)
- [DHCPv6 Local Server on page 742](#)
- [Configuration Statements on page 750](#)
- [Configuration Statements \(System\) on page 838](#)

### USB Modems for Remote Management Setup

- [Example: Configuring a USB Modem Interface on page 699](#)
- [Example: Configuring a Dialer Interface on page 702](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 705](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 707](#)

#### Example: Configuring a USB Modem Interface

This example shows how to configure a USB modem interface for dial backup.

- [Requirements on page 700](#)
- [Overview on page 700](#)

- [Configuration on page 700](#)
- [Verification on page 701](#)

### 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.

```
set interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
set modem-options init-command-string "ATS0=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*.

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 "ATS0=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 : ATSO=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 679](#)
- [USB Modem Interface Overview on page 676](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 705](#)
- *Administration Guide for Security Devices*
- *Modem Interfaces Feature Guide for Security Devices*

---

### Example: Configuring a Dialer Interface

This example shows how to configure a logical dialer interface for the device.

- [Requirements on page 702](#)
- [Overview on page 702](#)
- [Configuration on page 703](#)
- [Verification on page 704](#)

#### **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.

```
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 dl0 extensive** command. The output shows a summary of dialer interface information.

```
Physical interface: dl0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 24, Generation: 129
Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
Device flags      : Present Running
Interface flags: SNMP-Traps
Link type        : Full-Duplex
Link flags       : Keepalives
Physical info    : Unspecified
Hold-times       : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Last flapped     : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes      :          13859          0 bps
Output bytes     :           0          0 bps
Input packets    :           317          0 pps
Output packets   :           0          0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
```

```

Logical interface dl0.0 (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 676](#)
- [USB Modem Configuration Overview on page 679](#)
- [Example: Configuring a USB Modem Interface on page 699](#)
- [Example: Configuring a Dialer Interface for USB Modem Dial-In on page 705](#)
- *Administration Guide for Security Devices*

#### 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 706](#)
- [Overview on page 706](#)
- [Configuration on page 706](#)
- [Verification on page 707](#)

### 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 dl0.

### 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 dl0 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 dl0
```

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 dlo** command.

### **Related Documentation**

- [USB Modem Configuration Overview on page 679](#)
- [Example: Configuring a USB Modem Interface on page 699](#)
- *Administration Guide for Security Devices*
- *Modem Interfaces Feature Guide for Security Devices*

---

### **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 676](#)
- [USB Modem Configuration Overview on page 679](#)
- [Connecting to the Device Remotely on page 921](#)
- *Administration Guide for Security Devices*

## DHCP for IP Address Device

- [Example: Configuring the Device as a DHCP Server on page 709](#)
- [Example: Configuring the Device as a DHCP Client on page 714](#)
- [Example: Configuring the Device as a BOOTP or DHCP Relay Agent on page 718](#)
- [Configuring a DHCP Local Server on page 723](#)
- [Configuring a DHCP Client on page 727](#)
- [Configuring a DHCP Relay Agent on page 729](#)
- [Minimum DHCP Local Server Configuration on page 730](#)
- [Configuring Address-Assignment Pools on page 731](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 731](#)
- [Configuring DHCP Client-Specific Attributes on page 732](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 732](#)
- [Configuring Static Address Assignments on page 733](#)
- [Enabling TCP/IP Propagation on a DHCP Local Server on page 734](#)
- [Minimum DHCP Client Configuration on page 734](#)
- [Configuring Optional DHCP Client Attributes on page 735](#)
- [Minimum DHCP Relay Agent Configuration on page 736](#)

### Example: Configuring the Device as a DHCP Server

This example shows how to configure the device as a DHCP server.

- [Requirements on page 709](#)
- [Overview on page 709](#)
- [Configuration on page 709](#)
- [Verification on page 712](#)

#### 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.

```
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*.

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 712](#)
- [Verifying the DHCP Binding Database on page 712](#)
- [Verifying DHCP Server Operation on page 713](#)

### **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: mylablab.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 684](#)
- [Understanding DHCP Server Operation on page 686](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- *Administration Guide for Security Devices*

---

**Example: Configuring the Device as a DHCP Client**

---

This example shows how to configure the device as a DHCP client.

- [Requirements on page 714](#)
- [Overview on page 715](#)
- [Configuration on page 715](#)
- [Verification on page 717](#)

**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 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

#### 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 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 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. Set the DHCP lease time in seconds. From the Lease time list, select **Enter Specific Value**.

11. In the Length box, type **86400**.
12. Set the retransmission number of attempts. In the Retransmission attempt box, type **6**.
13. Set the retransmission interval in seconds. In the Retransmission interval box, type **5**.
14. Set the IPv4 address of the preferred DHCP server. In the Server address box, type **10.1.1.1**.
15. Set the vendor class ID. In the Vendor id box, type **ether**.
16. Click **OK**.
17. Click **OK** to check your configuration and save it as a candidate configuration.
18. 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 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. Set the DHCP lease time.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp]  
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]  
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]  
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]  
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]  
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;
  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 717](#)

### **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 684](#)
  - [Understanding DHCP Server Operation on page 686](#)
  - [Understanding DHCP Client Operation on page 687](#)
  - [DHCP Settings and Restrictions Overview on page 688](#)
  - *Administration Guide for Security Devices*

---

### 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 719](#)
- [Overview on page 719](#)
- [Configuration on page 719](#)
- [Verification on page 722](#)



### 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.

```
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*.

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 684](#)
- [Understanding DHCP Relay Agent Operation on page 687](#)
- [DHCP Settings and Restrictions Overview on page 688](#)
- *Administration Guide for Security Devices*

### Configuring a DHCP Local Server

- [Minimum DHCP Local Server Configuration on page 723](#)
- [Configuring Address-Assignment Pools on page 724](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 724](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 725](#)
- [Configuring Static Address Assignments on page 725](#)
- [Configuring DHCP Client-Specific Attributes on page 726](#)
- [Verifying and Managing DHCP Local Server Configuration on page 726](#)

#### Minimum DHCP Local Server Configuration

This 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 bob, and the DHCP local server is enabled on interface ge-1/0/1.0 within the group.

```
[edit access]
address-assignment {
  pool verizon family inet {
    network 192.168.1.0/24;
  }
}

edit system services
dhcp-local-server {
  group bob {
    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.

### **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 724.](#)
2. (Optional) Configure named ranges (subsets) of addresses.  
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 725.](#)
3. (Optional; IPv4 only) Create static address bindings.  
See [“Configuring Static Address Assignments” on page 725.](#)
4. (Optional) Configure attributes for DHCP clients.  
See [“Configuring DHCP Client-Specific Attributes” on page 726.](#)

### **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.

### *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.

### *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.

### Configuring DHCP Client-Specific Attributes

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.

### 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>`

### Configuring a DHCP Client

- [Minimum DHCP Client Configuration on page 727](#)
- [Configuring Optional DHCP Client Attributes on page 727](#)
- [Verifying and Managing DHCP Client Configuration on page 728](#)

#### 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.

#### 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, 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. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

3. 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
```

4. 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
```

5. 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
```

6. 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.

### *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>`

## Configuring a DHCP Relay Agent

- [Minimum DHCP Relay Agent Configuration on page 729](#)
- [Verifying and Managing DHCP Relay Configuration on page 729](#)

### 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 1.1.1.1/24. 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 {
  group bob {
    interface ge-1/0/1.0
  }
  server-group server-1 {
    address 1.1.1.1/24
  }
  active-server-group server-1
}
```



**NOTE:** To configure the DHCP relay agent in a routing instance, configure the `dhcp-relay` statements in the `[edit routing-instances]` hierarchy level .

### 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
```



**NOTE:** 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>`

### Minimum DHCP Local Server Configuration

This 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 bob, and the DHCP local server is enabled on interface ge-1/0/1.0 within the group.

```
[edit access]
address-assignment {
  pool verizon family inet {
    network 192.168.1.0/24;
  }
}

edit system services
dhcp-local-server {
  group bob {
    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 724](#)
- *Administration Guide for Security Devices*

## 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 724](#).
2. (Optional) Configure named ranges (subsets) of addresses.  
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 725](#).
3. (Optional;IPv4 only) Create static address bindings.  
See [“Configuring Static Address Assignments” on page 725](#).
4. (Optional) Configure attributes for DHCP clients.  
See [“Configuring DHCP Client-Specific Attributes” on page 726](#).

### Related Documentation

- *Administration Guide for Security Devices*

## 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 724](#)
- *Administration Guide for Security Devices*

## Configuring DHCP Client-Specific Attributes

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 724](#)
- *Administration Guide for Security Devices*

## 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 724](#)
- *Administration Guide for Security Devices*

### 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 724](#)
- *Administration Guide for Security Devices*

## 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**

- *Administration Guide for Security Devices*

## 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 727](#)
- *Administration Guide for Security Devices*

### 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, 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. Set the DHCP lease time.  

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```
3. 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
```
4. 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
```
5. 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
```
6. 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 727](#)
- *Administration Guide for Security Devices*

### 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 1.1.1.1/24. 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 {
  group bob {
    interface ge-1/0/1.0
  }
  server-group server-1 {
    address 1.1.1.1/24
  }
  active-server-group server-1
}
```



**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 729](#)
- *Administration Guide for Security Devices*

### DHCPv6 Client

- [Minimum DHCPv6 Client Configuration on page 736](#)
- [Configuring Optional DHCPv6 Client Attributes on page 737](#)
- [Configuring Nontemporary Address Assignment on page 738](#)
- [Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation on page 739](#)
- [Configuring Auto-Prefix Delegation on page 739](#)
- [Configuring the DHCPv6 Client Rapid Commit Option on page 740](#)
- [Configuring a DHCPv6 Client in Autoconfig Mode on page 741](#)
- [Configuring TCP/IP Propagation on a DHCPv6 Client on page 741](#)

### 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 693](#)

### 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.

#### Related Documentation

- [Minimum DHCPv6 Client Configuration on page 736](#)

### 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 736](#)

### 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 736](#)

### 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 736](#)
- [Configuring Optional DHCPv6 Client Attributes on page 737](#)

---

### 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 693](#)

### 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 736](#)
- [Configuring Optional DHCPv6 Client Attributes on page 737](#)

### 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 693](#)
- [Minimum DHCPv6 Client Configuration on page 736](#)

## DHCPv6 Local Server

- [Creating a Security Policy for DHCPv6 on page 742](#)
- [Example: Configuring DHCPv6 Server Options on page 743](#)
- [Example: Configuring an Address-Assignment Pool on page 745](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 748](#)
- [Configuring Address-Assignment Pool Linking on page 748](#)
- [Configuring DHCP Client-Specific Attributes on page 749](#)
- [Configuring an Address-Assignment Pool for Router Advertisement on page 750](#)

### 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 694](#)
- [Example: Configuring DHCPv6 Server Options on page 743](#)
- [Example: Configuring an Address-Assignment Pool on page 745](#)
- *Administration Guide for Security Devices*



### Example: Configuring DHCPv6 Server Options

This example shows how to configure DHCPv6 server options.

- [Requirements on page 743](#)
- [Overview on page 743](#)
- [Configuration on page 743](#)
- [Verification on page 745](#)

#### 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.

```
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*.

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

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify that the client address bindings and statistics for the DHCPv6 local server have been configured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Action</b>                | <p>From operational mode, enter these commands:</p> <ul style="list-style-type: none"> <li>• <b>show dhcpv6 server binding</b> command to display the address bindings in the client table on the DHCPv6 local server.</li> <li>• <b>show dhcpv6 server statistics</b> command to display the DHCPv6 local server statistics.</li> <li>• <b>clear dhcpv6 server bindings all</b> command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance.</li> <li>• <b>clear dhcpv6 server statistics</b> command to clear all DHCPv6 local server statistics.</li> </ul> |
| <b>Related Documentation</b> | <ul style="list-style-type: none"> <li>• <a href="#">DHCPv6 Server Overview on page 694</a></li> <li>• <a href="#">Example: Configuring an Address-Assignment Pool on page 745</a></li> <li>• <a href="#">Configuring a Named Address Range for Dynamic Address Assignment on page 748</a></li> <li>• <a href="#">Creating a Security Policy for DHCPv6 on page 742</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                      |

### Example: Configuring an Address-Assignment Pool

This example shows how to configure an address-assignment pool.

- [Requirements on page 746](#)
- [Overview on page 746](#)

- [Configuration on page 746](#)
- [Verification on page 747](#)

### 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.

```
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*.

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 694](#)
- [Example: Configuring DHCPv6 Server Options on page 743](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 748](#)
- [Creating a Security Policy for DHCPv6 on page 742](#)
- [Administration Guide for Security Devices](#)

### 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

- *Administration Guide for Security Devices*

### 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**

- *Administration Guide for Security Devices*

### 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 98 on page 749 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

**Table 98: DHCPv6 Attributes**

| Attribute                     | Description                                                      | DHCPv6 Option |
|-------------------------------|------------------------------------------------------------------|---------------|
| <b>dns-server</b>             | IPv6 address of DNS server to which clients can send DNS queries | 23            |
| <b>grace-period</b>           | Grace period offered with the lease                              | —             |
| <b>maximum-lease-time</b>     | Maximum lease time allowed by the DHCPv6 server                  | —             |
| <b>option</b>                 | User-defined options                                             | —             |
| <b>sip-server-address</b>     | IPv6 address of SIP outbound proxy server                        | 22            |
| <b>sip-server-domain-name</b> | Domain name of the SIP outbound proxy server                     | 21            |

**Related  
Documentation**

- *Administration Guide for Security Devices*

### 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**

- *Administration Guide for Security Devices*

### Configuration Statements

- [\[edit security certificates\] Hierarchy Level on page 752](#)
- [\[edit security ssh-known-hosts\] Hierarchy Level on page 752](#)
- [Interfaces Configuration Statement Hierarchy on page 753](#)
- [Groups Configuration Statement Hierarchy on page 768](#)
- [address-assignment \(Access\) on page 769](#)
- [address-pool \(Access\) on page 772](#)
- [allow-configuration on page 773](#)
- [allow-configuration-regexps on page 774](#)
- [authentication-key on page 775](#)
- [authentication-order on page 776](#)
- [boot-server \(NTP\) on page 777](#)
- [broadcast on page 778](#)
- [broadcast-client on page 779](#)
- [client-ia-type on page 779](#)
- [client-identifier \(dhcp-client\) on page 780](#)
- [client-identifier \(dhcpv6-client\) on page 780](#)
- [client-list-name \(SNMP\) on page 781](#)
- [client-type on page 781](#)
- [deny-configuration on page 782](#)
- [deny-configuration-regexps on page 783](#)
- [dhcp-attributes \(Access IPv4 Address Pools\) on page 784](#)
- [dhcp-attributes \(Access IPv6 Address Pools\) on page 786](#)



- [dhcp-client](#) on page 787
- [dhcpv6-client](#) on page 788
- [dhcp-local-server](#) (System Services) on page 789
- [dhcpv6](#) (System Services) on page 793
- [family](#) (Security Forwarding Options) on page 797
- [forwarding-options](#) (Security) on page 798
- [group](#) (System Services DHCP) on page 799
- [host](#) (SSH Known Hosts) on page 802
- [hostkey-algorithm](#) on page 803
- [interface](#) (System Services DHCP) on page 804
- [interfaces](#) (ARP) on page 805
- [interfaces](#) (Security Zones) on page 806
- [interface-traceoptions](#) (System Services DHCP) on page 807
- [internet-options](#) on page 809
- [lease-time](#) (dhcp-client) on page 810
- [lockout-period](#) on page 811
- [multicast-client](#) on page 811
- [name-server](#) (Access) on page 812
- [neighbor-discovery-router-advertisement](#) (Access) on page 812
- [ntp](#) on page 813
- [overrides](#) (System Services DHCP) on page 814
- [peer](#) (NTP) on page 815
- [port](#) (System Services Reverse SSH) on page 816
- [port](#) (System Services Reverse Telnet) on page 816
- [prefix](#) on page 817
- [profilerd](#) on page 818
- [proxy](#) on page 819
- [rapid-commit](#) on page 819
- [reconfigure](#) (System Services DHCP) on page 820
- [req-option](#) on page 821
- [retransmission-attempt](#) (dhcp-client) on page 822
- [retransmission-attempt](#) (dhcpv6-client) on page 822
- [retransmission-interval](#) (dhcp-client) on page 823
- [ssh](#) (reverse) on page 823
- [ssh-known-hosts](#) on page 824
- [server](#) (NTP) on page 825
- [server-address](#) (dhcp-client) on page 826

- [services](#) on page 827
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\)](#) on page 832
- [telnet \(System Services Reverse\)](#) on page 832
- [traceoptions \(System Services DHCP\)](#) on page 833
- [trusted-key](#) on page 835
- [update-router-advertisement](#) on page 835
- [update-server \(dhcp-client\)](#) on page 836
- [update-server \(dhcpv6-client\)](#) on page 836
- [user-id](#) on page 836
- [use-interface](#) on page 837
- [vendor-id](#) on page 837
- [vpn \(Forwarding Options\)](#) on page 838

---

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

---

```
security {
  certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority profile-name {
      ca-name name;
      crl filename;
      encoding (binary | pem);
      enrollment-url url;
      file filename;
      ldap-url url;
    }
    enrollment-retry number;
    local name {
      certificate;
      load-key-file url;
    }
    maximum-certificates number;
    path-length length;
  }
}
```

#### Related Documentation

- [Security Configuration Statement Hierarchy](#) on page 58
- *Administration Guide for Security Devices*
- *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 58](#)
- [Administration Guide for Security Devices](#)

### 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 {
          subrate value;
        }
        kentrox {
          subrate 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;
    (cbits-parity | no-cbits-parity);
    compatibility-mode {
        adtran {
            subrate value;
        }
    }
    digital-link {

```

```

        substrate value;
    }
    kentrox {
        substrate value;
    }
    larscom;
        substrate value;
    }
    verilink;
        substrate 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 output-policer-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**
- *Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices*
  - *Junos OS Interfaces Library for Security Devices*
  - *Administration Guide for Security Devices*

### 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*

## 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 Feature Guide for SRX Series Gateway Devices*
- *Administration Guide for Security Devices*

## address-pool (Access)

---

**Syntax**    address-pool *pool-name* {  
                  (address *address-or-address-prefix* ) {  
                    address-range {  
                      high *upper-limit*;  
                      low *lower-limit*;  
                      mask *network-mask*;  
                    }  
                  primary-dns *name*;  
                  primary-wins *name*;  
                  secondary-dns *name*;  
                  secondary-wins *name*;  
                }

**Hierarchy Level**    [edit access]

**Release Information**    Statement introduced in Release 10.4 of Junos OS.

**Description**    Create an address-pool for L2TP clients.

- Options**
- **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**    • *Administration Guide for Security Devices*

---

## allow-configuration

---

|                                 |                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>allow-configuration "regular-expression";</code>                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit system login class <i>class-name</i> ]                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.2 for SRX Series devices.                                                                                      |
| <b>Description</b>              | Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the <b>permissions</b> statement do not grant such access by default.                           |
| <b>Default</b>                  | If you omit this statement and the <b>deny-configuration</b> statement, users can edit only those commands for which they have access privileges through the <b>permissions</b> statement.                      |
| <b>Options</b>                  | <i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2.<br>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">System Configuration Statement Hierarchy on page 215</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                               |

## allow-configuration-regexps

---

|                                 |                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>allow-configuration-regexps "regular expression 1" "regular expression 2";</code>                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit system login class class-name]</code>                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 11.2 for SRX Series devices.                                                                                                                                                                                        |
| <b>Description</b>              | <p>Explicitly allow configuration access to specified hierarchies using regular expressions even if the permissions set with the <b>permissions</b> statement allow that access.</p> <p>The statement <b>deny-configuration-regexps</b> takes precedence if it is used in the same login class definition.</p> |
| <b>Default</b>                  | If you do not configure this statement or the <b>deny-configuration-regexps</b> statement, users can edit only those commands for which they have access privileges set with the <b>permissions</b> statement.                                                                                                 |
| <b>Options</b>                  | <i>regular expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2.<br>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.                                                                                                |
| <b>Required Privilege Level</b> | <code>system</code> —To view this statement in the configuration.<br><code>system-control</code> —To add this statement to the configuration.                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">System Configuration Statement Hierarchy on page 215</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                              |



## authentication-key

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>authentication-key <i>key-number</i> type <i>md5</i> value &lt;<i>password</i>&gt;;</code>                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <code>[edit system <i>ntp</i>]</code>                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <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> |
| <b>Options</b>                  | <p><b><i>key-number</i></b>—Positive integer that identifies the key.</p> <p><b><i>type md5</i></b>—Authentication type. It can only be <b><i>md5</i></b>.</p> <p><b><i>value password</i></b>—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</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="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                  |

## authentication-order

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>authentication-order [ <i>authentication-methods</i> ];</code>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit <a href="#">system</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure 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.                                                                                                                                                                                                                                             |
| <b>Default</b>                  | If you do not include the <b>authentication-order</b> statement, users are verified based on their configured passwords.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <b><i>authentication-methods</i></b> —One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following: <ul style="list-style-type: none"><li>• <b>password</b>—Use the password configured for the user with the <b>authentication</b> statement at the [edit <b>system login user</b>] hierarchy level.</li><li>• <b>radius</b>—Use RADIUS authentication services.</li><li>• <b>tacplus</b>—Use TACACS+ authentication services.</li></ul> |
| <b>Required Privilege Level</b> | <b>system</b> —To view this statement in the configuration.<br><b>system-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                  |

## boot-server (NTP)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>boot-server (address   hostname);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit system ntp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <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 <b>ntpdate</b> 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 <b>ntpdate</b> 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> |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>address</b>—The IP address of an NTP boot server.</li> <li>• <b>hostname</b>—The hostname of an NTP boot server.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## broadcast

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>broadcast address &lt;key key-number&gt; &lt;routing-instance-name routing-instance-name&gt; &lt;ttl value&gt; &lt;version value&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit system <i>ntp</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>address</b>—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 <b>224.0.1.1</b>.</p> <p><b>key key-number</b>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p><b>Range:</b> Any unsigned 32-bit integer</p> <p><b>routing-instance-name routing-instance-name</b>—(Optional) The routing instance name in which the interface has an address in the broadcast subnet.</p> <p><b>Default:</b> The default routing instance is used to broadcast packets.</p> <p><b>ttl value</b>—(Optional) Time-to-live (TTL) value to use.</p> <p><b>Range:</b> 1 through 255</p> <p><b>Default:</b> 1</p> <p><b>version value</b>—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p><b>Range:</b> 1 through 4</p> <p><b>Default:</b> 4</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="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## broadcast-client

---

|                                 |                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>broadcast-client;</code>                                                                                                                  |
| <b>Hierarchy Level</b>          | <code>[edit system <i>ntp</i>]</code>                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                               |
| <b>Description</b>              | Configure the SRX Series device to listen for broadcast messages on the local network to discover other servers on the same subnet.             |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul> |

## client-ia-type

---

|                                 |                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-ia-type (ia-na   ia-pd);</code>                                                                                     |
| <b>Hierarchy Level</b>          | <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]</code>          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                            |
| <b>Description</b>              | Configure the DHCPv6 client identity association type.                                                                           |
| <b>Options</b>                  | <p><b>ia-na</b>—Identity association for nontemporary address</p> <p><b>ia-pd</b>—Identity association for prefix delegation</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                             |

## client-identifier (dhcp-client)

---

|                                 |                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | client-identifier {<br>user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i> ;<br>use-interface-description {logical   device};<br>prefix [host-name routing-instance-name];<br>} |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                  |
| <b>Description</b>              | The DHCP server identifies a client by a client-identifier value.                                                                                                                      |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                     |

## client-identifier (dhcpv6-client)

---

|                                 |                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | client-identifier duid-type (duid-ll   duid-llt   vendor);                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                                                                                  |
| <b>Description</b>              | The DHCPv6 server identifies a client by a client-identifier value.                                                                                                                                                                                                    |
| <b>Options</b>                  | <b>duid-type</b> —The DHCPv6 client is identified by a DHCP unique identifier (DUID).<br><br><b>duid-ll</b> —Link Layer address.<br><br><b>duid-llt</b> —Link Layer address plus time.<br><br><b>vendor</b> —Vendor-assigned unique ID based on the enterprise number. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                     |

## client-list-name (SNMP)

|                                 |                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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 Release 8.5 of Junos OS.                                                                                                                                                                                                         |
| <b>Description</b>              | 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. |
| <b>Options</b>                  | <i>client-list-name</i> — Name of the client list. Client list is the list of IP address prefixes defined with the <b>prefix-list</b> statement in the policy-options hierarchy.                                                                         |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                     |

## client-type

|                                 |                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>client-type (autoconfig   statefull);</code>                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                            |
| <b>Description</b>              | The type of DHCPv6 client.                                                                                                                                                       |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• autoconfig—Autoconfig client type for router advertisement</li> <li>• statefull— Stateful client type for address assignment</li> </ul> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                             |

## deny-configuration

---

|                                 |                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>deny-configuration "regular-expression";</code>                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit system login class]                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 11.2 for SRX Series devices.                                                                                          |
| <b>Description</b>              | Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the <b>permissions</b> statement grant such access by default.                                       |
| <b>Default</b>                  | If you omit this statement and the <b>allow-configuration</b> statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the <b>permissions</b> statement. |
| <b>Options</b>                  | <b>regular-expression</b> —Extended (modern) regular expression as defined in POSIX 1003.2.<br>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.     |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">System Configuration Statement Hierarchy on page 215</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                   |



## deny-configuration-regexps

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>deny-configuration-regexps "regular expression 1" "regular expression 2";</code>                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit system login class <i>class-name</i> ]                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 11.2 for SRX Series devices.                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Explicitly deny configuration access to specified hierarchies using regular expressions even if the permissions set with the <b>permissions</b> statement allow that access.</p> <p>Expressions configured with this statement take precedence over <b>allow-configuration-regexps</b> if the two statements are used in the same login class definition.</p> |
| <b>Default</b>                  | If you do not configure this statement or the <b>deny-configuration-regexps</b> statement, users can edit only those commands for which they have access privileges set with the <b>permissions</b> statement.                                                                                                                                                   |
| <b>Options</b>                  | <p><i>regular expression</i>—Extended (modern) regular expression as defined in POSIX 1003.2.</p> <p>If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.</p>                                                                                                                                        |
| <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="#">System Configuration Statement Hierarchy on page 215</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                             |

## 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]

|                                 |                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Release Information</b>      | Statement introduced in Release 10.4 of Junos OS.                                                                                                          |
| <b>Description</b>              | Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options. |
| <b>Required Privilege Level</b> | access—To view this statement in the configuration.<br>access-control—To add this statement to the configuration.                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                         |

## 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 Release 10.4 of Junos OS.

**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** • *Administration Guide for Security Devices*

## 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.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • *Administration Guide for Security Devices*

## dhcpv6-client

---

**Syntax**    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 *number*;  
              update-router-advertisement {  
                  interface *interface-name*;  
              }  
              update-server;  
          }

**Hierarchy Level**    [edit interfaces *interface-name* unit *logical-unit-number* family *family*]

**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 options are explained separately.

**Required Privilege Level**    interface—To view this statement in the configuration.  
                                  interface-control—To add this statement to the configuration.

**Related Documentation**    • *Administration Guide for Security Devices*

## 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 Release 10.4 of Junos OS.

**Description** Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.



**NOTE:** SRX Series and J Series devices do not support client authentication.

**Options** The remaining statements are explained separately.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- *Administration Guide for Security Devices*

## dhcpv6 (System Services)

```
Syntax  dhcpv6 {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        group group-name {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
            dynamic-profile {
                profile-name;
                aggregate-clients {
                    merge;
                    replace;
                }
                junos-default-profile;
                use-primary dynamic-profile;
            }
        }
    }
```

```
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
}
overrides {
  delegated-pool pool-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit ;
}
reconfigure {
```

```

        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
        }
        version (0 | 1 | automatic);
    }
}
overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit ;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
service-profile service-profile-name;
}

```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Release 10.4 of Junos OS.

**Description** Configure DHCPv6 server to provide IPv6 addresses to clients.



**NOTE:** SRX Series and J Series devices do not support client authentication.

---

**Options**

- **duplicate-clients-on-interface**—Allow duplicate clients on different interfaces in a subnet.

Remaining options 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**

- *Administration Guide for Security Devices*

## 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 Release 8.5 of Junos OS.

**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.

**Required Privilege Level**

|                                                              |
|--------------------------------------------------------------|
| security—To view this statement in the configuration.        |
| security-control—To add this statement to the configuration. |

**Related Documentation**

- *MPLS Feature Guide for Security Devices*
- *Administration Guide for Security Devices*

## 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 Release 8.5 of Junos OS.

**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.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *MPLS Feature Guide for Security Devices*
- *Administration Guide for Security Devices*
- *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 Release 10.4 of Junos OS.

**Description** Configure a group of interfaces that have a common configuration. The remaining statements are explained separately.

**Options**    • *group-name*—Name of the group.



**NOTE:** SRX Series and J Series devices do not support DHCP client authentication.

---

The remaining statements are explained separately.


|                              |                                                            |
|------------------------------|------------------------------------------------------------|
| <b>Required Privilege</b>    | access—To view this statement in the configuration.        |
| <b>Level</b>                 | access-control—To add this statement to the configuration. |
| <b>Related Documentation</b> | • <i>Administration Guide for Security Devices</i>         |

## host (SSH Known Hosts)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>host <i>hostname</i> {<br/>    dsa-key <i>dsa-key</i>;<br/>    ecdsa-sha2-nistp256-key <i>ecdsa-sha2-nistp256-key</i>;<br/>    ecdsa-sha2-nistp384-key <i>ecdsa-sha2-nistp384-key</i>;<br/>    ecdsa-sha2-nistp521-key <i>ecdsa-sha2-nistp521-key</i>;<br/>    rsa-key <i>rsa-key</i>;<br/>    rsa1-key <i>rsa1-key</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit security ssh-known-hosts]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement modified in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Configure the type of base-64 encoded host key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b><i>hostname</i></b>—Name of the SSH known host.</li><li>• <b><i>dsa-key dsa-key</i></b>—Digital Signature Algorithm (DSA) for SSH version 2</li><li>• <b><i>ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key</i></b>—Elliptic Curve Digital Signature Algorithm (ECDSA)</li><li>• <b><i>ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key</i></b>—Elliptic Curve Digital Signature Algorithm (ECDSA)</li><li>• <b><i>ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key</i></b>—Elliptic Curve Digital Signature Algorithm (ECDSA)</li><li>• <b><i>rsa-key rsa-key</i></b>—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2</li><li>• <b><i>rsa1-key rsa1-key</i></b>—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1</li></ul> |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## hostkey-algorithm

|                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                      | <pre>hostkey-algorithm {   (ssh-dss   no-ssh-dss);   (ssh-ecdsa   no-ssh-ecdsa);   (ssh-rsa   no-ssh-rsa); }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                                                                             | [edit system services ssh]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>                                                                                                                                                                                                         | <p>Statement introduced in Release 11.2 of Junos OS.</p> <p>Statement options modified in Release 12.2 of Junos OS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>                                                                                                                                                                                                                 | Allow or disallow a host-key signature algorithm for the SSH host to use to authenticate another host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• <b>ssh-dss</b>—Allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.</li> <li>• <b>no-ssh-dss</b>—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.</li> <li>• <b>ssh-ecdsa</b>—Allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.</li> <li>• <b>no-ssh-ecdsa</b>—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.</li> <li>• <b>ssh-rsa</b>—Allow generation of a 2048-bit RSA host-key.</li> <li>• <b>no-ssh-rsa</b>—Do not allow generation of a 2048-bit RSA host-key.</li> </ul> |
| <div>  <p><b>NOTE:</b> DSA keys are not supported in FIPS, so the ssh-dss option is not available on systems operating in FIPS mode.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## interface (System Services DHCP)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interface <i>interface-name</i> {<br/>    exclude;<br/>    overrides {<br/>        interface-client-limit <i>number</i>;<br/>    }<br/>    trace;<br/>    upto <i>upto-interface-name</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | 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.                                                                                                                                                                           |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <i>interface-name</i>—Name of the interface.</li><li>• <b>trace</b>—Enable tracing of the interface specified by the <i>interface-name</i> argument.</li><li>• <b>upto</b> <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>.</li></ul> |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                             |

---

## interfaces (ARP)

---

|                                 |                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interfaces {<br/>    <i>interface-name</i> {<br/>        aging-timer <i>minutes</i>;<br/>    }<br/>}</pre>                             |
| <b>Hierarchy Level</b>          | [edit system arp]                                                                                                                           |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 9.4.                                                                                           |
| <b>Description</b>              | Specify the Address Resolution Protocol (ARP) aging timer in minutes for a logical interface.                                               |
| <b>Options</b>                  | <p><b>aging-timer <i>minutes</i></b>—Time between ARP updates, in minutes.</p> <p><b>Range:</b> 1 through 240</p> <p><b>Default:</b> 20</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>Junos OS Administration Library for Security Devices</i></li></ul>                               |

## interfaces (Security Zones)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>interfaces <i>interface-name</i> {<br/>    host-inbound-traffic {<br/>        protocols <i>protocol-name</i> {<br/>            except;<br/>        }<br/>    system-services <i>service-name</i> {<br/>        except;<br/>    }<br/>}</pre>                                                                                                          |
| <b>Hierarchy Level</b>          | [edit security zones functional-zone management],<br>[edit security zones security-zone <i>zone-name</i> ]                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Specify the set of interfaces that are part of the zone.                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <i>interface-name</i> —Name of the interface.<br><br>The remaining statements are explained separately.                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Ethernet Port Switching Feature Guide for Security Devices</i></li><li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li><li>• <i>Security Zones and Interfaces Feature Guide for Security Devices</i></li><li>• <i>Administration Guide for Security Devices</i></li></ul> |



## interface-traceoptions (System Services DHCP)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> interface-traceoptions {     file {         filename ;         files number;         match regular-expression;         size maximum-file-size;         (world-readable   no-world-readable);     }     flag flag;     level (all   error   info   notice   verbose   warning);     no-remote-trace; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],<br>[edit system services dhcp-local-server]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b> | Statement introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>         | Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the <b>interface <i>interface-name</i> trace</b> statement at the [edit system services group <i>group-name</i> ] hierarchy level to enable the tracing operation on the specific interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>             | <p><b>file-name</b>—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 <b>jdhcpd</b> in the directory <b>/var/log</b>. If you include the <b>file</b> statement, you must specify a filename.</p> <p><b>files number</b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag flag</b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all events</li> <li>• <b>dhcpv6-packet</b>—Trace DHCPv6 packet decoding operations.</li> <li>• <b>dhcpv6-packet-option</b>—Trace DHCPv6 option decoding operations.</li> <li>• <b>dhcpv6-state</b>—Trace changes in state for DHCPv6 operations.</li> <li>• <b>packet</b>—Trace packet decoding operations</li> <li>• <b>packet-option</b>—Trace DHCP option decoding operations</li> <li>• <b>state</b>—Trace changes in state</li> </ul> |

**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.

|                                 |                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| <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>Administration Guide for Security Devices</i></li></ul> |

## 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**

- *Administration Guide for Security Devices*

---

## lease-time (dhcp-client)

---

**Syntax** lease-time *seconds*;

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcp-client]

**Release Information** Statement introduced in Junos OS Release 12.1X44-D10.

**Description** Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

**Options** **seconds**— Request time to negotiate and exchange information.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**

- *Administration Guide for Security Devices*

## lockout-period

---

|                                 |                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | lockout-period <i>minutes</i> ;                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit system login retry-options]                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                |
| <b>Description</b>              | 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 <b>tries-before-disconnect</b> statement. |
| <b>Options</b>                  | <i>minutes</i> —Amount of time before the user can attempt to log in after being locked out.<br><b>Default:</b> 120<br><b>Range:</b> 1 through 43200                                                          |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                          |

## multicast-client

---

|                                 |                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | multicast-client < <i>address</i> >;                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit system ntp]                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                |
| <b>Description</b>              | For NTP, configure the SRX Series device to listen for multicast messages on the local network to discover other servers on the same subnet.                     |
| <b>Options</b>                  | <i>address</i> —(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups.<br><b>Default:</b> 224.0.1.1. |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                  |

## name-server (Access)

---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>name-server address;</code>                                                                                 |
| <b>Hierarchy Level</b>          | [edit access address-assignment pool <i>pool-name</i> family (inet   inet6) xauth-attributes]                     |
| <b>Release Information</b>      | Statement introduced in Release 10.4 of Junos OS.                                                                 |
| <b>Description</b>              | Specify the DNS server IP address for an address-assignment pool.                                                 |
| <b>Required Privilege Level</b> | access—To view this statement in the configuration.<br>access-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                |

## neighbor-discovery-router-advertisement (Access)

---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>neighbor-discovery-router-advertisement <i>ndra-pool-name</i>;</code>                                       |
| <b>Hierarchy Level</b>          | [edit access address-assignment]                                                                                  |
| <b>Release Information</b>      | Statement introduced in Release 10.4 of Junos OS.                                                                 |
| <b>Description</b>              | Configure the name of the address-assignment pool used to assign the router advertisement prefix.                 |
| <b>Options</b>                  | <i>ndra-pool-name</i> —Name of the address assignment pool.                                                       |
| <b>Required Privilege Level</b> | access—To view this statement in the configuration.<br>access-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                |

## ntp

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> ntp {   authentication-key <i>key-number</i> type <i>md5</i> value &lt;password&gt;;   boot-server &lt;address&gt;;   broadcast &lt;address&gt; &lt;key <i>key-number</i>&gt; &lt;routing-instance <i>routing-instance-name</i>&gt; &lt;version     value&gt; &lt;ttl <i>value</i>&gt;;   broadcast-client;   multicast-client &lt;address&gt;;   peer <i>address</i> &lt;key <i>key-number</i>&gt; &lt;version <i>value</i>&gt; &lt;prefer&gt;;   server <i>address</i> &lt;key <i>key-number</i>&gt; &lt;version <i>value</i>&gt; &lt;prefer&gt;;   source-address <i>source-address</i> &lt;routing-instance <i>routing-instance-name</i>&gt;;   trusted-key [<i>key-numbers</i>]; }</pre> |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | <p>Configure Network Time Protocol (NTP) on the SRX Series device.</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="#">System Configuration Statement Hierarchy on page 215</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## overrides (System Services DHCP)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>overrides {   interface-client-limit <i>number</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | <p>Override the default configuration settings for the extended DHCP local server. Specifying the <b>overrides</b> statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.</p> <ul style="list-style-type: none"> <li>To override global DHCP local server configuration options, include the <b>overrides</b> statement and its subordinate statements at the <b>[edit system services dhcp-local-server]</b> hierarchy level.</li> <li>To override configuration options for a named group of interfaces, include the statements at the <b>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]</b> hierarchy level.</li> <li>To override configuration options for a specific interface within a named group of interfaces, include the statements at the <b>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>]</b> hierarchy level.</li> <li>Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.</li> </ul> |
| <b>Options</b>                  | <p><b>interface-client-limit <i>number</i></b>—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><b>Range:</b> 1 through 500,000</p> <p><b>Default:</b> No limit</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>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



## peer (NTP)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>peer address &lt;key key-number&gt; &lt;version value&gt; &lt;prefer&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit system ntp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | 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.                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>address</b>—Address of the remote system. You must specify an address, not a hostname.</p> <p><b>key key-number</b>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p><b>Range:</b> Any unsigned 32-bit integer</p> <p><b>prefer</b>—(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><b>version value</b>—(Optional) Specify the NTP version number to be used in outgoing NTP packets.</p> <p><b>Range:</b> 1 through 4</p> <p><b>Default:</b> 4</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="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## port (System Services Reverse SSH)

---

|                                 |                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | port <i>port-number</i> ;                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit system services reverse ssh ]                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Release 9.6 of Junos OS.                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Reverse SSH allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2901 is used. |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                               |

## port (System Services Reverse Telnet)

---

|                                 |                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | port <i>port-number</i> ;                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit system services reverse telnet]                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Release 9.6 of Junos OS.                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. You can control the port that is used. By default, port 2900 is used. |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                  |

---

## prefix

---

|                                 |                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>prefix {<br/>    host-name;<br/>    logical-system-name;<br/>    routing-instance-name;<br/>}</pre>                   |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                      |
| <b>Description</b>              | Specify a prefix as a client identifier.                                                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                         |

## profilerd

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <pre>profilerd {<br/>    command <i>binary-file-path</i>;<br/>    disable;<br/>    failover (alternate-media   other-routing-engine);<br/>}</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"><li>• <b>command <i>binary-file-path</i></b>—Path to binary for process.</li><li>• <b>disable</b>—Disable the profiler 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.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Related Documentation    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## proxy

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> proxy {     password <i>password</i>;     port <i>port-number</i>;     server <i>url</i>;     username <i>user-name</i>; } </pre>                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Specify the proxy information for the router.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>password <i>password</i></b>—Password configured in the proxy server.</li> <li>• <b>port <i>port number</i></b>—Proxy server port number.<br/>Range: 0 through 65,535</li> <li>• <b>server <i>url</i></b>—URL or IP address of the proxy server host.</li> <li>• <b>username <i>username</i></b>—Username configured in the proxy server.</li> </ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                             |

## rapid-commit

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | rapid-commit;                                                                                                           |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                   |
| <b>Description</b>              | Used to signal the use of the two-message exchange for address assignment.                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                    |

## reconfigure (System Services DHCP)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> reconfigure {     attempts <i>number</i>;     clear-on-abort;     strict;     timeout <i>number</i>;     token <i>token-name</i>;     trigger {         radius-disconnect;     } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>     | <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>         | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>             | <p><b>attempts <i>number</i></b>—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><b>Range:</b> 1 through 10 attempts</p> <p><b>Default:</b> 8 attempts</p> <p><b>clear-on-abort</b>—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><b>strict</b>—Configure the system to only allow packets that contain the reconfigure accept option.</p> <p><b>timeout <i>seconds</i></b>—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><b>Range:</b> 1 through 10 seconds</p> <p><b>Default:</b> 2 seconds</p> <p><b>token <i>token-name</i></b>—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** • *Administration Guide for Security Devices*

## req-option

**Syntax** req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);

**Hierarchy Level** [edit interfaces *interface-name* unit *logical-unit-number* family *family* dhcpv6-client]

**Release Information** Statement introduced in Junos OS Release 12.1X45-D10.

**Description** The configuration options requested by the DHCPv6 client.

**Options** **dns-server**—Specify a DNS server.

**domain**—Specify a domain name.

**fqdn**—Specify a fully qualified domain name.

**nis-domain**—Specify a Network Information Service (NIS) domain.

**nis-server**—Specify a Network Information Service (NIS) server.

**ntp-server**—Specify a Network Time Protocol (NTP) server.

**sip-domain**—Specify a Session Initiation Protocol (SIP) domain.

**sip-server**—Specify a Session Initiation Protocol (SIP) server.

**time-zone**—Specify a time zone.

**vendor-spec**—Specify vendor specification.

**Required Privilege Level** interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation** • *Administration Guide for Security Devices*

## retransmission-attempt (dhcp-client)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | retransmission-attempts <i>number</i> ;                                                                                 |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                   |
| <b>Description</b>              | Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.   |
| <b>Options</b>                  | <b>number</b> —Number of attempts to retransmit the packet.<br><b>Range:</b> 0 through 6                                |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                      |

## retransmission-attempt (dhcpv6-client)

---

|                                 |                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | retransmission-attempt <i>number</i> ;                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                     |
| <b>Description</b>              | 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. |
| <b>Options</b>                  | <b>number</b> —Number of retransmit attempts                                                                                                                                                              |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                        |



## retransmission-interval (dhcp-client)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>retransmission-interval seconds;</code>                                                                           |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                   |
| <b>Description</b>              | Specify the time between successive retransmission attempts.                                                            |
| <b>Options</b>                  | <b>seconds</b> —Number of seconds between successive retransmission attempts.<br><b>Range:</b> 4 through 64 seconds     |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                    |

## ssh (reverse)

---

|                                 |                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ssh port <i>port-number</i>;</code>                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system services reverse]                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Release 9.6 of Junos OS.                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. Use reverse SSH to encrypt the reverse telnet communication between the device and the client. |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                         |

## ssh-known-hosts

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <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> |
| <b>Hierarchy Level</b>          | [edit security]                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement modified in Release 8.5 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Configure SSH support for known hosts and for administering SSH host key updates.                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>fetch-from-server <i>server-name</i></b>—Retrieve SSH public host key information from a specified server.</li> <li>• <b>load-key-file <i>key-file</i></b>—Import SSH host-key information from the specified <code>/var/tmp/ssh-known-hosts</code> file.</li> </ul> <p>The remaining statements are explained separately</p>                                      |
| <b>Required Privilege Level</b> | <p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                           |

## server (NTP)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>server address &lt;key key-number&gt; &lt;version value&gt; &lt;prefer&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit system ntp]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <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>     |
| <b>Options</b>                  | <p><b>address</b>—Address of the remote system. You must specify an address, not a hostname.</p> <p><b>key key-number</b>—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.</p> <p><b>Range:</b> Any unsigned 32-bit integer</p> <p><b>prefer</b>—(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><b>version value</b>—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p><b>Range:</b> 1 through 4</p> <p><b>Default:</b> 4</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="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## server-address (dhcp-client)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | server address <i>ip-address</i> ;                                                                                      |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                   |
| <b>Description</b>              | Specify the preferred DHCP server address that is sent to DHCP clients.                                                 |
| <b>Options</b>                  | <b>ip-address</b> —DHCP server address.                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                      |

## 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;
    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 {
    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;
}
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+)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>source-address <i>source-address</i> &lt;routing-instance <i>routing-instance-name</i>&gt;;</code>                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit system accounting destination radius <i>server server-address</i> ],<br>[edit system accounting destination tacplus <i>server server-address</i> ],<br>[edit system <i>ntp</i> ],<br>[edit system <i>radius-server server-address</i> ],<br>[edit system <i>syslog</i> ],<br>[edit system <i>tacplus-server server-address</i> ]                                   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | 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.                                                                                                                                                                                 |
| <b>Options</b>                  | <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 <b>host <i>hostname</i></b> statements at the [edit system <b>syslog</b> ] hierarchy level, but not for messages directed to the other Routing Engine. |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">ntp on page 813</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                             |

## telnet (System Services Reverse)

---

|                                 |                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>telnet port <i>port-number</i>;</code>                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit system services reverse ]                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Release 9.6 of Junos OS.                                                                                                                                                                              |
| <b>Description</b>              | Reverse Telnet allows you to configure a device to listen on a specific port for telnet and SSH (secure shell) services. When you connect to that port, the device provides an interface to the auxiliary port on the device. |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                            |

## traceoptions (System Services DHCP)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> traceoptions {   file {     filename;     files number;     size maximum-file-size;     (world-readable   no-world-readable);   }   flag flag;   no-remote-trace; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>     | <pre> [edit routing-instances routing-instance-name system services dhcp-local-server], [edit system services dhcp-local-server] [edit system processes dhcp-service] </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b> | Statement introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>         | Configure extended DHCP local server tracing operations for DHCP processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>             | <ul style="list-style-type: none"> <li>• <b>file-name</b>—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 <b>jdhcpd</b> in the directory <b>/var/log</b>. If you include the <b>file</b> statement, you must specify a filename.</li> <li>• <b>files number</b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, 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 <b>size</b> option.</li> </ul> <p><b>Range:</b> 2 through 1000<br/> <b>Default:</b> 3 files</p> <ul style="list-style-type: none"> <li>• <b>match regular-expression</b>—(Optional) Refine the output to include lines that contain the regular expression.</li> <li>• <b>size maximum-file-size</b>—(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 <b>files</b> option.</li> </ul> <p><b>Syntax:</b> <b>xk</b> to specify KB, <b>xm</b> to specify MB, or <b>xg</b> to specify GB<br/> <b>Range:</b> 10 KB through 1 GB<br/> <b>Default:</b> 128 KB</p> <ul style="list-style-type: none"> <li>• <b>world-readable</b>—(Optional) Enable unrestricted file access.</li> <li>• <b>no-world-readable</b>—(Optional) Disable unrestricted file access.</li> <li>• <b>flag flag</b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags: <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all events.</li> </ul> </li> </ul> |

- **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**    • *Administration Guide for Security Devices*

## trusted-key

---

|                                 |                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>trusted-key [key-numbers];</code>                                                                                                                |
| <b>Hierarchy Level</b>          | [edit system <i>ntp</i> ]                                                                                                                              |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.                                                                                                      |
| <b>Description</b>              | 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. |
| <b>Options</b>                  | <b>key-numbers</b> —One or more key numbers. Each key can be any 32-bit unsigned integer except 0.                                                     |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">ntp on page 813</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>        |

## update-router-advertisement

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>update-router-advertisement (interface <i>interface-name</i>);</code>                                             |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                   |
| <b>Description</b>              | Specify the interface used to delegate prefixes.                                                                        |
| <b>Options</b>                  | <b>interface <i>interface-name</i></b> —Interface on which to delegate prefixes                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                    |

## update-server (dhcp-client)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | update-server;                                                                                                          |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                   |
| <b>Description</b>              | Propagate DHCP options to a local DHCP server.                                                                          |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                      |

## update-server (dhcpv6-client)

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | update-server;                                                                                                          |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcpv6-client]              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                   |
| <b>Description</b>              | Propagate TCP/IP settings to the DHCPv6 server.                                                                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                      |

## user-id

---

|                                 |                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | user-id {ascii <i>ascii</i> hexadecimal <i>hexadecimal</i> };                                                              |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                      |
| <b>Description</b>              | Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.                         |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                         |

## use-interface

---

|                                 |                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>use-interface-description {logical   device};</code>                                                                 |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client client-identifier] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                      |
| <b>Description</b>              | The description configured at the physical or logical interface level is used for client identification.                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                       |

## vendor-id

---

|                                 |                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>vendor-id <i>vendor-id</i>;</code>                                                                                |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> dhcp-client]                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                   |
| <b>Description</b>              | Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.                                  |
| <b>Options</b>                  | <b>vendor-id</b> —Vendor class ID.                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                    |

## vpn (Forwarding Options)

---

|                                 |                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | vpn;                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit forwarding-options helpers bootp]<br>[edit forwarding-options helpers bootp interface <i>interface-name</i> ]                                                                   |
| <b>Release Information</b>      | Statement introduced in Release 9.0 of Junos OS.                                                                                                                                      |
| <b>Description</b>              | 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. |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                    |

## Configuration Statements (System)

- [System Configuration Statement Hierarchy on page 839](#)
- [ciphers on page 870](#)
- [connection-limit on page 871](#)
- [disable \(System Services\) on page 872](#)
- [dlv on page 872](#)
- [kernel-replication \(System\) on page 873](#)
- [location on page 874](#)
- [macs on page 875](#)
- [protocol-version on page 876](#)
- [radius-server on page 877](#)
- [root-authentication on page 878](#)
- [single-connection on page 879](#)
- [static-subscribers on page 879](#)
- [statistics-service on page 880](#)
- [subscriber-management on page 880](#)
- [subscriber-management-helper on page 881](#)
- [uac-service on page 882](#)
- [usb-control on page 883](#)
- [watchdog on page 883](#)
- [web-management on page 884](#)
- [web-management \(System Services\) on page 885](#)



## 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 J Series and 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;
}
}
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;
}
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 {
        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**


- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *Firewall User Authentication Feature Guide for Security Devices*
- *Infranet Authentication Feature Guide for Security Devices*
- *Installation and Upgrade Guide for Security Devices*

## ciphers

|                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                          | <code>ciphers [ cipher-1 cipher-2 cipher-3 ...]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                 | <code>[edit system services ssh]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>                                                                                                                                                                                                                             | Statement introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>                                                                                                                                                                                                                                     | Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                                                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>• <b>3des-cbc</b>—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.</li> <li>• <b>aes128-cbc</b>—128-bit Advanced Encryption Standard (AES) in CBC mode.</li> <li>• <b>aes256-cbc</b>—256-bit AES in CBC mode.</li> <li>• <b>aes128-ctr</b>—128-bit AES in CBC mode.</li> <li>• <b>aes192-ctr</b>—192-bit AES in counter mode.</li> <li>• <b>aes256-ctr</b>—256-bit AES in counter Mode.</li> <li>• <b>arcfour128</b>—128-bit RC4-stream cipher in CBC mode.</li> <li>• <b>arcfour256</b>—256-bit RC4-stream cipher in CBC mode.</li> <li>• <b>blowfish128-cbc</b>—128-bit blowfish-symmetric block cipher in CBC mode.</li> <li>• <b>cast128-cbc</b>—128-bit cast in CBC mode.</li> </ul> |
| <div>  <p><b>NOTE:</b> Ciphers represent a set. To configure ssh ciphers:</p> <pre>user@host#set system services ssh ciphers [ aes256-cbc aes192-cbc ]</pre> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <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>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



## connection-limit

|                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                     | connection-limit <i>limit</i> ;                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                            | [edit system services finger]<br>[edit system services ftp]<br>[edit system services netconf ssh]<br>[edit system services ssh]<br>[edit system services telnet]<br>[edit system services xnm-clear-text]<br>[edit system services xnm-ssl]                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                        | Statement introduced in Junos OS Release 11.4.                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                                                                                                                | 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).                                                                                                                                                                    |
| <b>Options</b>                                                                                                                                                                                                                                                                                                    | <p><b>limit</b>—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:<br/> <b>Range:</b> 1 through 250<br/> <b>Default:</b> 75</p> <p>On all branch SRX Series devices, the range is as follows:<br/> <b>Range:</b> 1 through 5</p> |
| <div>  <p><b>NOTE:</b> 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> |                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                   | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• <a href="#">System Configuration Statement Hierarchy on page 215</a></li> </ul>                                                                                                                                                                                                                           |

## disable (System Services)

---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | disable;                                                                                                          |
| <b>Hierarchy Level</b>          | [edit system services dns dnssec]                                                                                 |
| <b>Release Information</b>      | Statement introduced in Release 10.2 of Junos OS.                                                                 |
| <b>Description</b>              | Disables DNSSEC in the DNS server.                                                                                |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                |

## dlv

---

|                                 |                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | dlv {<br>domain-name <i>domain-name</i> trusted-anchor <i>trusted-anchor</i> ;<br>}                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system services dns dnssec]                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Release 10.2 of Junos OS.                                                                                                                                                      |
| <b>Description</b>              | Configure DNSSEC Lookaside Validation (DLV).                                                                                                                                                           |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• domain-name <i>domain-name</i>—Specify the secure domain server name.</li><li>• trusted-anchor <i>trusted-anchor</i>—Specify the trusted DLV anchor.</li></ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                     |

## kernel-replication (System)


---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | kernel-replication;                                                                                               |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1.                                                                    |
| <b>Description</b>              | Configure kernel replication.                                                                                     |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                |

## location

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the physical location of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>altitude <i>feet</i></b>—Number of feet above sea level.</li> <li>• <b>building <i>name</i></b>—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 (" ").</li> <li>• <b>country-code <i>code</i></b>—Two-letter country code.</li> <li>• <b>floor <i>number</i></b>—Floor number in the building.</li> <li>• <b>hcoord <i>horizontal-coordinate</i></b>—Bellcore Horizontal Coordinate.</li> <li>• <b>lata <i>service-area</i></b>—Long-distance service area.</li> <li>• <b>latitude <i>degrees</i></b>—Latitude in degree format.</li> <li>• <b>longitude <i>degrees</i></b>—Longitude in degree format.</li> <li>• <b>npa-nxx <i>number</i></b>—First six digits of the phone number (area code and exchange).</li> <li>• <b>postal-code <i>postal-code</i></b>—Zip code or Postal code.</li> <li>• <b>rack <i>number</i></b>—Rack number.</li> <li>• <b>vcoord <i>vertical-coordinate</i></b>—Bellcore Vertical Coordinate.</li> </ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## macs

|                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                 | <code>macs [algorithm]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                        | <code>[edit system services ssh]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                    | Statement introduced in Release 11.2 of Junos OS.<br>SHA-2 options introduced in Release 12.1 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                                                                                                            | Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• <code>hmac-md5</code>—Hash-based MAC using Message-Digest 5 (MD5).</li> <li>• <code>hmac-md5-96</code>—96-bits of Hash-based MAC using MD5.</li> <li>• <code>hmac-ripemd160</code>—Hash-based MAC using RIPEMD.</li> <li>• <code>hmac-sha1</code>—Hash-based MAC using Secure Hash Algorithm (SHA-1).</li> <li>• <code>hmac-sha1-96</code>—96-bits of Hash-based MAC using SHA-1.</li> <li>• <code>hmac-sha2-256</code>—256-bits of Hash-based MAC using SHA-2.</li> <li>• <code>hmac-sha2-256-96</code>—first 96-bits of hmac-sha2-256.</li> <li>• <code>hmac-sha2-512</code>—96-bits of Hash-based MAC using SHA-1.</li> <li>• <code>umac-64</code>—Message Authentication Code using Universal Hashing.</li> </ul> |
| <div>  <p><b>NOTE:</b> 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> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                               | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## protocol-version

---

|                                 |                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>protocol-version <i>version</i>;</code>                                                                     |
| <b>Hierarchy Level</b>          | [edit system services ssh]                                                                                        |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 11.4.                                                                |
| <b>Description</b>              | Specify the SSH protocol versions supported.                                                                      |
| <b>Default</b>                  | v2—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.                                    |
| <b>Options</b>                  | <b><i>version</i></b> —SSH protocol version: v1, v2, or both.                                                     |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">hostkey-algorithm on page 803</a></li></ul>                   |

## radius-server

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>radius-server server-address {     accounting-port <i>port-number</i>;     port <i>port-number</i>;     retry <i>value</i>;     secret <i>password</i>;     max-outstanding-requests <i>value</i>;     source-address <i>source-address</i>;     timeout <i>seconds</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>     | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b> | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>         | <p>Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP).</p> <p>To configure multiple RADIUS servers, include multiple <b>radius-server</b> statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>             | <ul style="list-style-type: none"> <li><b>server-address</b>—Address of the RADIUS server.</li> <li><b>accounting-port <i>port-number</i></b>—RADIUS server accounting port number.<br/> <b>Range:</b> 1 through 65,335 files<br/> <b>Default:</b> 1813</li> <li><b>port <i>port-number</i></b>—RADIUS server authentication port number.<br/> <b>Range:</b> 1 through 65,335 files<br/> <b>Default:</b> 1812</li> <li><b>retry <i>value</i></b>—Number of times that the router is allowed to attempt to contact a RADIUS server.<br/> <b>Range:</b> 1 through 10<br/> <b>Default:</b> 3</li> <li><b>secret <i>password</i></b>—Password to use; it can include spaces if the character string is enclosed in quotation marks.</li> <li><b>max-outstanding-requests <i>value</i></b>—Maximum number of outstanding requests in flight to server.<br/> <b>Range:</b> 1 through 65,335 files</li> <li><b>source-address <i>source-address</i></b>—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.</li> <li><b>timeout <i>seconds</i></b>—Amount of time to wait.</li> </ul> |

**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**

- *Administration Guide for Security Devices*

---

## root-authentication

---

**Syntax** 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*>;  
    }  
}

**Hierarchy Level** [edit system]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify authentication information for the root login.

- Options**
- **encrypted-password *password***—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 *URL***—File URL containing one or more SSH keys.
  - **ssh-dsa *public-key***—SSH DSA public key string.
    - **from *pattern-list***—Pattern list of allowed hosts.
  - **ssh-rsa *public-key***—SSH RSA public key string.
    - **from *pattern-list***—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**

- *Administration Guide for Security Devices*



## single-connection

---

|                                 |                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | single-connection;                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit system accounting destination tacplus server <i>server-address</i> ]<br>[edit system tacplus-server <i>server-address</i> ]                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                     |
| <b>Description</b>              | 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. |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">System Configuration Statement Hierarchy on page 215</a></li> </ul>                                                                          |

## static-subscribers

---

|                                 |                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | static-subscribers {<br>disable;<br>}                                                                                      |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                              |
| <b>Description</b>              | Associate subscribers with statically configured interfaces, and provide dynamic service activation for these subscribers. |
| <b>Options</b>                  | <b>disable</b> —Disable the static subscribers process.                                                                    |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                       |

## statistics-service

---

|                                 |                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>statistics-service {<br/>    command <i>binary-file-path</i>;<br/>    disable;<br/>}</pre>                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                   |
| <b>Description</b>              | Specify the Packet Forwarding Engine (PFE) statistics service management process.                                                                                                                                               |
| <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 Packet Forwarding Engine (PFE) statistics service management process.</li></ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                              |

## subscriber-management

---

|                                 |                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>subscriber-management {<br/>    command <i>binary-file-path</i>;<br/>    disable;<br/>}</pre>                                                                                       |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                            |
| <b>Description</b>              | Specify the subscriber management process.                                                                                                                                               |
| <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 subscriber management process.</li></ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                       |

## subscriber-management-helper

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | subscriber-management-helper {<br>command <i>binary-file-path</i> ;<br>disable;<br>failover (alternate-media   other-routing-engine);<br>}                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Specify the subscriber management helper process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <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 subscriber management helper 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> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## uac-service

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>uac-service {<br/>    command <i>binary-file-path</i>;<br/>    disable;<br/>    failover (alternate-media   other-routing-engine);<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Specify the unified access control daemon process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <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 unified access control daemon 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> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <i>Firewall User Authentication Feature Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## usb-control

---

|                                 |                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | usb-control {<br>command <i>binary-file-path</i> ;<br>disable;<br>}                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                              |
| <b>Description</b>              | Specify the universal serial bus (USB) supervise process.                                                                                                                                                  |
| <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 universal serial bus (USB) supervise process.</li> </ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                       |

## watchdog

---

|                                 |                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | watchdog {<br>disable;<br>enable;<br>timeout <i>value</i> ;<br>}                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                      |
| <b>Description</b>              | Enable or disable the watchdog timer when Junos OS encounters a problem.                                                                                                                                                                                                           |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>disable</b>—Disable the watchdog timer.</li> <li>• <b>enable</b>—Enable the watchdog timer.</li> <li>• <b>timeout <i>value</i></b>—Specify amount of time to wait in seconds.<br/>    <b>Range:</b> 1 through 3600 seconds.</li> </ul> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                               |

## web-management

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>web-management {<br/>  disable;<br/>  failover (alternate-media   other-routing-engine);<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system processes]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Specify the Web management process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b>disable</b>—Disable the Web management 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> |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## 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 Feature Guide for Security Devices*
- *Administration Guide for Security Devices*
- *Firewall User Authentication Feature Guide for Security Devices*
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*

## Administration

---

- [Secure Web Access on page 888](#)
- [User Authentication and Access on page 894](#)
- [USB Modems for Remote Management Setup on page 921](#)
- [Telnet and SSH Device Control on page 922](#)
- [DHCP for IP Address Device on page 930](#)
- [File Management on page 932](#)
- [Licenses on page 938](#)
- [Operational Commands on page 946](#)

## Secure Web Access

- [Generating an SSL Certificate Using the openssl Command on page 888](#)
- [Generating a Self-Signed SSL Certificate on page 889](#)
- [Manually Generating Self-Signed SSL Certificates on page 889](#)
- [Configuring Device Addresses on page 890](#)
- [Enabling Access Services on page 891](#)
- [Example: Configuring Secure Web Access on page 892](#)
- [Adding, Editing, and Deleting Certificates on the Device on page 894](#)

### 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

- *Administration Guide for Security Devices*

### 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

- *Administration Guide for Security Devices*

### 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**

- *Administration Guide for Security Devices*

---

### 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**

- *Administration Guide for Security Devices*

## 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

- *Administration Guide for Security Devices*

## Example: Configuring Secure Web Access

This example shows how to configure secure Web access on your device.

- [Requirements on page 892](#)
- [Overview on page 892](#)
- [Configuration on page 892](#)
- [Verification on page 893](#)

### 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.

```
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
      qPwbTiOkJvqoDw2YgYseOZ5zzVJyErgSg954T\nEuHM67Ck8hAOrcnb0YO+SY
      Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
      ... KYiFf4CbBBbjlMQJOHFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
      eIQBdp1UjziYf7NuzDx4Z\n -----END RSA PRIVATE KEY-----\n-----BEGIN
      CERTIFICATE----- \nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
      FADCBKTELMAkGA1UEBhMCdXMx\nCzAJBgNVBAGTAhMhMRlWYAYDVQQHEwZldW5ue
      HBIYnMxDTALBgNVBAMTBGpucHlxJDAiBgkqhkiG\n9w0BCQEWFW5iaGFyZ2F2YUB
      fLUYAnBYmsYWOH\n -----END CERTIFICATE-----\n"; ## SECRET-DATA
    }
  }
}
```

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

### Verification

Confirm that the configuration is working properly.

- [Verifying an SSL Certificate Configuration on page 893](#)
- [Verifying a Secure Access Configuration on page 893](#)

### 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 663](#)
- [Generating an SSL Certificate Using the openssl Command on page 888](#)
- [Generating a Self-Signed SSL Certificate on page 889](#)
- [Configuring Device Addresses on page 890](#)
- *Junos OS Interfaces Library for Security Devices*

---

**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**

- *Administration Guide for Security Devices*

**User Authentication and Access**

- [Example: Configuring a RADIUS Server for System Authentication on page 895](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 897](#)
- [Example: Configuring Authentication Order on page 900](#)
- [Example: Configuring New Users on page 902](#)
- [Example: Configuring System Retry Options on page 905](#)
- [Example: Creating Template Accounts on page 908](#)
- [Handling Authorization Failure on page 911](#)



- [Understanding Administrative Roles on page 912](#)
- [Example: Configuring Administrative Roles on page 914](#)

### Example: Configuring a RADIUS Server for System Authentication

This example shows how to configure a RADIUS server for system authentication.

- [Requirements on page 895](#)
- [Overview on page 895](#)
- [Configuration on page 895](#)
- [Verification on page 897](#)

#### 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.

```
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*.

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 900](#).
- Configure a user. See [“Example: Configuring New Users” on page 902](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 908](#).

### **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 671](#)
- [Understanding User Accounts on page 672](#)
- [Example: Configuring a TACACS+ Server for System Authentication on page 897](#)
- [Understanding Login Classes on page 673](#)
- *Administration Guide for Security Devices*

### **Example: Configuring a TACACS+ Server for System Authentication**

This example shows how to configure a TACACS+ server for system authentication.

- [Requirements on page 897](#)
- [Overview on page 898](#)
- [Configuration on page 898](#)
- [Verification on page 899](#)

### **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.

```
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 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*.

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 900](#).
- Configure a user. See [“Example: Configuring New Users” on page 902](#).
- Configure local user template accounts. See [“Example: Creating Template Accounts” on page 908](#).

### Verification

Confirm that the configuration is working properly.

#### Verifying the TACACS+ Server System Authentication Configuration

**Purpose** Verify that the TACACS+ server has been configured for system authentication.

**Action** From operational mode, enter the **show system tacplus-server** command.

**Related Documentation**

- [Understanding User Authentication Methods on page 671](#)
- [Understanding User Accounts on page 672](#)
- [Example: Configuring a RADIUS Server for System Authentication on page 895](#)
- [Understanding Login Classes on page 673](#)
- [Administration Guide for Security Devices](#)

## Example: Configuring Authentication Order

---

This example shows how to configure authentication order.

- [Requirements on page 900](#)
- [Overview on page 900](#)
- [Configuration on page 900](#)
- [Verification on page 901](#)

### Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

### Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

### Configuration

#### CLI Quick Configuration

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

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

#### GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Authentication Method and Order** tab.
4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
  - RADIUS
  - TACACS+
  - Local Password

If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.

5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.
6. Click **OK** to check your configuration and save it as a candidate configuration.
7. If you are done configuring the device, click **Commit Options>Commit**.

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

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 895.
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication”](#) on page 897.
- Configure a user. See [“Example: Configuring New Users”](#) on page 902.
- Configure template accounts. See [“Example: Creating Template Accounts”](#) on page 908.

#### 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 671](#)
  - [Understanding User Accounts on page 672](#)
  - [Understanding Login Classes on page 673](#)
  - *Administration Guide for Security Devices*

---

**Example: Configuring New Users**

---

This example shows how to configure new users.

- [Requirements on page 902](#)
- [Overview on page 902](#)
- [Configuration on page 903](#)
- [Verification on page 904](#)

***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.

```
set system login class operator-and-boot allow-commands "request system reboot"
set system login class operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password
$1$ABC123
```

#### GUI Step-by-Step Procedure

To configure new users:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.
2. Click **Edit**. The Edit User Management dialog box appears.
3. Select the **Users** tab.

4. Click **Add** to add a new user. The Add User dialog box appears.

5. In the User name box, type a unique name for the user.

Do not include spaces, colons, or commas in the username.

6. In the User ID box, type a unique ID for the user.

7. In the Full Name box, type the user's full name.

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.

9. From the Login Class list, select the user's access privilege:

- **operator**
- **read-only**
- **unauthorized**

This list also includes any user-defined login classes.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.

11. Click **OK** to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click **Commit Options>Commit**.

#### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

```
[edit system login]
user@host# set class operator-and-boot allow-commands "request system reboot"
```

2. Set the permission bits for the login class.

```
[edit system login]
user@host# set class operator-and-boot permissions [clear network reset trace
view]
```

3. Set the username, login class, and encrypted password for the user.

```
[edit system login]
user@host# set user cmartin class superuser authentication encrypted-password
$1$ABC123
```

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

```
[edit]
user@host# show system login
class operator-and-boot {
permissions [ clear network reset trace view ];
allow-commands "request system reboot";
}
user cmartin {
class superuser;
authentication {
encrypted-password "$1$ABC123";
}
}
```

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



**NOTE:** To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See [“Example: Configuring a RADIUS Server for System Authentication” on page 895](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 897](#).
- Configure a user. See [“Example: Configuring New Users” on page 902](#).
- Configure template accounts. See [“Example: Creating Template Accounts” on page 908](#).

### 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 671](#)
  - [Understanding User Accounts on page 672](#)
  - [Understanding Template Accounts on page 676](#)
  - [Understanding Login Classes on page 673](#)
  - *Administration Guide for Security Devices*

---

### **Example: Configuring System Retry Options**

This example shows how to configure system retry options to protect the device from malicious users.

- [Requirements on page 905](#)
- [Overview on page 905](#)
- [Configuration on page 907](#)
- [Verification on page 908](#)

#### **Requirements**

Before you begin, you should understand “[Handling Authorization Failure](#)” on page 911.

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*.

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**

|                              |                                                                                                                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify that the login lockout configuration is enabled                                                                                                                                                                                                                                                             |
| <b>Action</b>                | 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 <b>show system login lockout</b> command.                                                                                   |
| <b>Meaning</b>               | 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 <b>show system login lockout</b> command. |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Handling Authorization Failure on page 911</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                            |

---

### **Example: Creating Template Accounts**

This example shows how to create template accounts.

- [Requirements on page 908](#)
- [Overview on page 908](#)
- [Configuration on page 909](#)
- [Verification on page 910](#)

#### **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 909](#)
- [Creating a Local Template Account on page 909](#)

#### **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*.

To create a remote template account:

1. 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*.

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 895](#).
- Configure a TACACS+ server. See [“Example: Configuring a TACACS+ Server for System Authentication” on page 897](#).
- Configure system authentication order. See [“Example: Configuring Authentication Order” on page 900](#).

### 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.

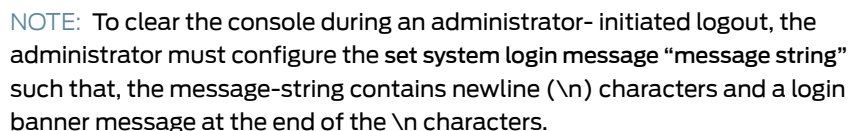
**Related Documentation**

- [Understanding User Authentication Methods on page 671](#)
- [Understanding User Accounts on page 672](#)
- [Understanding Login Classes on page 673](#)



- ## Handling Authorization Failure

The number of reattempts the device allows is defined by the **tries-before-disconnect** option. The device allows 3 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console.

[illegible]

**Related Documentation**

- [Example: Configuring System Retry Options on page 905](#)
- *Administration Guide for Security Devices*

---

### 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 914](#)

### 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 914](#)
- [Overview on page 914](#)
- [Configuration on page 914](#)
- [Verification on page 919](#)

#### 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.

```

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 lockout)|^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* in the Junos OS CLI guide.

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 lockout)|^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 lockout)|^file (copy|delete|rename)|^rollback|^set date|^show security
(alarms|dynamic-policies|match-policies|policies)|^start shell"
user@host# set allow-configuration-regexps "security (ike|ipsec) (policy|proposal)"
"security ipsec ^vpn$.* manual (authentication|encryption|protocol|spi)" "system
fips self-test after-key-generation"

```

```
user@host# set security-role crypto-administrator
```

5. Create the **security-admin** login class.

```
[edit]
user@host# set system login class security-admin
```

```
[edit system login class security-admin]
user@host# set permissions all
```

6. Configure the **security-admin** login class restrictions.

```
[edit system login class security-admin]
user@host# set deny-commands "^clear (log|security log)|^(clear|show) security
alarms alarm-type idp|^request (security|system
set-encryption-key)|^rollback|^start shell"
user@host# set deny-configuration-regexps "security alarms potential-violation
idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .* manual
(authentication| encryption|protocol|spi)" "security log cache" "security log
exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
user@host# set security-role security-administrator
```

7. Create the **ids-admin** login class.

```
[edit]
user@host# set system login class ids-admin
```

```
[edit system login class ids-admin]
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the **ids-admin** login class restrictions.

```
[edit system login class ids-admin]
user@host# set allow-configuration-regexps "security alarms potential-violation
idp" "security log exclude .* event-id IDP_.*"
set system login class ids-admin deny-commands "^clear log|^(clear|show) security
alarms (alarm-id|all|newer-than|older- than|process|severity)|^(clear|show)
security alarms alarm-type
(authentication|cryptographic-self-test|decryption-failures|encryption-failures|
ike-phase1-failures|ike-phase2-failures|key-generation-self-test|
non-cryptographic-self-test|policy|replay-attacks)|^file
(copy|delete|rename)|^request (security|system set-encryption-key)|
^rollback|^set date|^show security (dynamic-policies|match-policies|policies)|^start
shell"
set system login class ids-admin deny-configuration-regexps "security alarms
potential-violation (authentication|cryptographic-self-test|decryption-
failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
user@host# set security-role ids-administrator
```

9. Assign users to the roles.

```
[edit]
user@host# set system login
```

```
[edit system login]
user@host# set user audit-officer class audit-admin
user@host# set user crypto-officer class crypto-admin
user@host# set user security-officer class security-admin
user@host# set user ids-officer class ids-admin
```

10. Configure passwords for the users.

```
[edit system login]
user@host# set user audit-officer authentication plain-text-password
user@host# set user crypto-officer authentication plain-text-password
user@host# set user security-officer authentication plain-text-password
user@host# set user ids-officer authentication plain-text-password
```

### Results

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

```
[edit]
user@host# show system
system {
  login {
    class audit-admin {
      permissions [ maintenance security trace ];
      allow-commands "^clear (log|security log)";
      deny-commands "^clear (security alarms|system login logout)|^file
        (copy|delete|rename)|^request (security|system
          set-encryption-key)|^rollback|^set date|^show security
          (alarms|dynamic-policies|match-policies|policies)|^start shell";
      security-role audit-administrator;
    }
    class crypto-admin {
      permissions [ admin-control configure maintenance security-control system-control
        trace ];
      allow-commands "^request (system set-encryption-key)";
      deny-commands "^clear (log|security alarms|security log|system login logout)|^file
        (copy|delete|rename)|^rollback|^set date|^show security
        (alarms|dynamic-policies|match-policies|policies)|^start shell";
      allow-configuration-regexps "security (ike|ipsec) (policy|proposal)" "security ipsec
        ^vpn$ .* manual (authentication|encryption|protocol|spi)" "system fips self-test
        after-key-generation" ;
      security-role crypto-administrator;
    }
    class security-admin {
      permissions [ all];
      deny-commands "^clear (log|security log)|^(clear|show) security alarms alarm-type
        idp|^request (security|system set-encryption-key)|^rollback|^start shell";
      deny-configuration-regexps "security alarms potential-violation idp" "security
        (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .* manual
        (authentication|encryption|protocol|spi)" "security log exclude .* event-id IDP_.*"
        "system fips self-test after-key-generation";
      security-role security-administrator;
    }
    class ids-admin {
```



```

permissions [ configure maintenance security-control trace ];
deny-commands "^clear log|^ (clear|show) security alarms
    (alarm-id|all|newer-than|older-than|process|severity)|^ (clear|show) security
    alarms alarm-type
    (authentication | cryptographic-self-test | decryption-failures | encryption-failures
    | ike-phase1-failures | ike-phase2-failures|key-generation-self-test |
    non-cryptographic-self-test |policy | replay-attacks) | ^file (copy|delete|rename)
    | ^request (security|system set-encryption-key) | ^rollback |
    ^set date | ^show security (dynamic-policies|match-policies|policies) | ^start shell";
allow-configuration-regexps "security alarms potential-violation idp" "security log
    exclude .* event-id IDP_*";
deny-configuration-regexps "security alarms potential-violation
    (authentication|cryptographic-self-test|decryption-
    failures|encryption-failures|ike-phase1-failures|ike-phase2-failures|
    key-generation-self-test|non-cryptographic-self-test|policy|replay-attacks)"
security-role ids-administrator;
}
user audit-officer {
    class audit-admin;
    authentication {
        encrypted-password "$1$ABC123"; ## SECRET-DATA
    }
}
user crypto-officer {
    class crypto-admin;
    authentication {
        encrypted-password "$1$ABC123"; ## SECRET-DATA
    }
}
user security-officer {
    class security-admin;
    authentication {
        encrypted-password "$1$ABC123"; ##SECRET-DATA
    }
}
user ids-officer {
    class ids-admin;
    authentication {
        encrypted-password "$1$ABC123"; ## SECRET-DATA
    }
}
}
}

```

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

### **Verification**

Confirm that the configuration is working properly.

#### **Verifying the login permissions**

**Purpose** Verify the login permissions for the current user.

**Action** From operational mode, enter the **show cli authorization** command.

```

user@host>show cli authorization
Current user: '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
  storage     -- Can view fibre channel storage protocol configuration
  storage-control-- Can modify fibre channel storage protocol configuration
  all-control -- Can modify any configuration
Individual command authorization:
  Allow regular expression: none
  Deny regular expression: none
  Allow configuration regular expression: none
  Deny configuration regular expression: none

```

This output summarizes the login permissions.

**Related Documentation** • [Understanding Administrative Roles on page 912](#)

## USB Modems for Remote Management Setup

- [Connecting to the Device Remotely on page 921](#)
- [Modifying USB Modem Initialization Commands on page 921](#)
- [Resetting USB Modems on page 922](#)

### 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 676](#)
- [USB Modem Configuration Overview on page 679](#)
- [Configuring a Dial-Up Modem Connection Remotely on page 707](#)
- *Administration Guide for Security Devices*

### 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 676](#)
- [USB Modem Configuration Overview on page 679](#)
- [Resetting USB Modems on page 922](#)
- *Administration Guide for Security Devices*

---

### 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 676](#)
- [USB Modem Configuration Overview on page 679](#)
- [Modifying USB Modem Initialization Commands on page 921](#)
- *Administration Guide for Security Devices*

## Telnet and SSH Device Control

- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Configuring Reverse Telnet and Reverse SSH on page 924](#)

- [Example: Controlling Management Access on SRX and J-Series Devices on page 925](#)
- [The telnet Command on page 928](#)
- [The ssh Command on page 929](#)

### 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 928](#)
- [The ssh Command on page 929](#)
- [Reverse Telnet Overview on page 683](#)
- [Configuring Reverse Telnet and Reverse SSH on page 924](#)
- *Administration Guide for Security Devices*

---

### 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 928](#)
- [The ssh Command on page 929](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Reverse Telnet Overview on page 683](#)
- *Administration Guide for Security Devices*

### Example: Controlling Management Access on SRX and J-Series Devices

This example shows how to control management access on SRX Series devices.

- [Requirements on page 925](#)
- [Overview on page 925](#)
- [Configuration on page 925](#)
- [Verification on page 927](#)

#### 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 and J Series devices.

#### Configuration

- [Configuring an IP Address List to Restrict Management Access to a Device on page 925](#)

#### 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.

```
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*.

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**

- *Administration Guide for Security Devices*

## 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 99 on page 928 describes the **telnet** command options.

**Table 99: 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 source-interface</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 port</b>                              | Specify the port number or service name on the host.                                                                                                                                  |
| <b>routing-instance routing-instance-name</b> | Use the specified routing instance for the Telnet session.                                                                                                                            |
| <b>source address</b>                         | Use the specified source address for the Telnet session.                                                                                                                              |

### Related Documentation

- [The ssh Command on page 929](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Reverse Telnet Overview on page 683](#)

- [Configuring Reverse Telnet and Reverse SSH on page 924](#)
- *Administration Guide for Security Devices*

### 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 100 on page 929 describes the **ssh** command options.

**Table 100: 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 source-interface</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 routing-instance-name</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 928](#)
- [Configuring Password Retry Limits for Telnet and SSH Access on page 923](#)
- [Reverse Telnet Overview on page 683](#)
- [Configuring Reverse Telnet and Reverse SSH on page 924](#)

- *Administration Guide for Security Devices*

## DHCP for IP Address Device

- [Verifying and Managing DHCP Local Server Configuration on page 930](#)
- [Verifying and Managing DHCP Client Configuration on page 930](#)
- [Verifying and Managing DHCP Relay Configuration on page 931](#)

### 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**

- *Administration Guide for Security Devices*

### 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

- *Administration Guide for Security Devices*

### 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
```



**NOTE:** 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>`

**Related  
Documentation**

- *Administration Guide for Security Devices*

**File Management**

- [Decrypting Configuration Files on page 932](#)
- [Encrypting Configuration Files on page 932](#)
- [Modifying the Encryption Key on page 934](#)
- [Cleaning Up Files on page 934](#)
- [Cleaning Up Files with the CLI on page 935](#)
- [Deleting Files on page 936](#)
- [Deleting the Backup Software Image on page 937](#)
- [Downloading Files on page 937](#)
- [Managing Accounting Files on page 938](#)

---

**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 101 on page 933](#).

Table 101: request system set-encryption-key Commands

| CLI Command                                            | Description                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>request system set-encryption-key</b>               | Sets the encryption key and enables default configuration file encryption: <ul style="list-style-type: none"> <li>• AES encryption for the Canada and U.S. version of Junos OS</li> <li>• DES encryption for the international version of Junos OS</li> </ul>                                                                                    |
| <b>request system set-encryption-key algorithm des</b> | Sets the encryption key and specifies configuration file encryption by DES.                                                                                                                                                                                                                                                                      |
| <b>request system set-encryption-key unique</b>        | 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>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> |
| <b>request system set-encryption-key des unique</b>    | 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:example1
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:exampleone
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*

### 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*

## Licenses

- [Displaying License Keys on page 938](#)
- [Downloading License Keys on page 939](#)
- [Generating a License Key on page 939](#)
- [Saving License Keys on page 940](#)
- [Updating License Keys on page 941](#)
- [Example: Adding a New License Key on page 941](#)
- [Example: Deleting a License Key on page 945](#)

### Displaying License Keys

---

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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*
- *Administration Guide for Security Devices*

---

### 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*

---

### 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**

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*

---

### 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Displaying License Keys on page 254](#)

- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*

### 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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Example: Deleting a License Key on page 260](#)
- *Installation and Upgrade Guide for Security Devices*

### Example: Adding a New License Key

This example shows how to add a new license key.

- [Requirements on page 942](#)
- [Overview on page 942](#)
- [Configuration on page 942](#)
- [Verification on page 943](#)

### 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: G03000002223

License version: 2

Valid for device: JN001875AB

Features:

bgp-reflection - Border Gateway Protocol route reflection  
permanent

License identifier: G03000002225

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 944](#)
- [Verifying License Usage on page 944](#)
- [Verifying Installed License Keys on page 944](#)

**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 xxx
```

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 Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
  - [Generating a License Key on page 254](#)
  - [Updating License Keys on page 256](#)
  - [Saving License Keys on page 255](#)
  - [Displaying License Keys on page 254](#)
  - [Downloading License Keys on page 255](#)
  - [Example: Deleting a License Key on page 260](#)
  - [Installation and Upgrade Guide for Security Devices](#)

### Example: Deleting a License Key

This example shows how to delete a license key.

- [Requirements on page 945](#)
- [Overview on page 945](#)
- [Configuration on page 945](#)
- [Verification on page 946](#)

#### 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 G03000002223.

#### 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 G03000002223
```

##### 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 G03000002223
```



**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**

**Purpose** Verify that the expected licenses have been removed from the device.

**Action** From operational mode, enter the **show system license** command.

**Related Documentation**

- [Junos OS Feature License Model Number for J Series Services Routers and SRX Series Services Gateways on page 159](#)
- [Generating a License Key on page 254](#)
- [Updating License Keys on page 256](#)
- [Saving License Keys on page 255](#)
- [Displaying License Keys on page 254](#)
- [Downloading License Keys on page 255](#)
- [Example: Adding a New License Key on page 257](#)
- [Installation and Upgrade Guide for Security Devices](#)

## **Operational Commands**

- [clear dhcp client binding](#)
- [clear dhcpv6 client binding](#)
- [clear dhcp client statistics](#)
- [clear dhcpv6 client statistics](#)
- [clear dhcp relay binding](#)
- [clear dhcp relay statistics](#)
- [clear dhcp server binding](#)
- [clear dhcp server statistics](#)
- [clear dhcpv6 server binding \(Local Server\)](#)
- [clear dhcpv6 server statistics \(Local Server\)](#)
- [clear system login logout](#)
- [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 partition compact-flash
- 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 reboot
- request system software rollback (Maintenance)
- request support information
- request system zeroize
- restart (Reset)
- Restart Commands Overview on page 1011
- show chassis routing-engine (View)
- show dhcp client binding
- show dhcpv6 client binding
- show dhcp client statistics
- show dhcpv6 client statistics
- show dhcp relay binding
- show dhcp relay statistics

- [show dhcp server binding](#)
- [show dhcp server 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

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp client binding<br>[all interface <interface-name>]<br>[routing-instance <routing-instance-name>]                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>all</b>—(Optional) Clear the binding state for all DHCP clients.</p> <p><b>interface &lt;interface-name&gt;</b>—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p><b>routing-instance &lt;routing-instance-name&gt;</b>—(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> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcp client binding on page 1014</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## clear dhcpv6 client binding

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcpv6 client binding<br>[all   interface <i>interface-name</i> ]<br>[routing-instance <i>routing-instance-name</i> ]                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>all</b>—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p><b>routing-instance <i>routing-instance-name</i></b>—(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> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcpv6 client binding on page 1017</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



---

## clear dhcp client statistics

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp client statistics<br><all><br><interface><br><routing-instance>                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>all</b>—(Optional) Clear all the DHCP client statistics.</p> <p><b>interface</b>—(Optional) Clear the statistics for DHCP clients on the specified interface.</p> <p><b>routing-instance</b> —(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> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcp client statistics on page 1019</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                          |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                               |

## clear dhcpv6 client statistics

---

|                                 |                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcpv6 client statistics<br>routing-instance <i>routing-instance-name</i>                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                                                          |
| <b>Description</b>              | Clear all DHCPv6 client statistics.                                                                                                                                                                                                            |
| <b>Options</b>                  | <b>routing-instance <i>routing-instance-name</i></b> —(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. |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcpv6 client statistics on page 1021</a></li></ul>                                                                                                                                   |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                               |

## clear dhcp relay binding

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp relay binding<br><all   ip-address   mac-address><br><interface interface-name><br><routing-instance routing-instance-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <p><b>all</b>—(Optional) Clear the binding state for all DHCP clients.</p> <p><b>ip-address</b>— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p><b>mac-address</b>—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p><b>interface interface-name</b>—(Optional) Clear the binding state for DHCP clients on the specified interface</p> <p><b>routing-instance routing-instance-name</b>—(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> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcp relay binding on page 1023</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## clear dhcp relay statistics

---

|                                 |                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp relay statistics<br><routing-instance routing-instance-name>                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                |
| <b>Description</b>              | Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.                                                                                                                                                               |
| <b>Options</b>                  | <b>routing-instance routing-instance-name</b> —(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. |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcp relay statistics on page 1025</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                 |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                     |

## clear dhcp server binding

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp server binding<br><all   ip-address   mac-address><br><interface interface-name><br><routing-instance routing-instance-name>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>all</b>—(Optional) Clear the binding state for all DHCP clients.</p> <p><b>ip-address</b>— (Optional) Clear the binding state for the DHCP client, using the specified IP address.</p> <p><b>mac-address</b>—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.</p> <p><b>interface interface-name</b>—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p><b>routing-instance routing-instance-name</b>—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcp server binding on page 1027</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## clear dhcp server statistics

---

|                                 |                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp server statistics<br><routing-instance routing-instance-name>                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                 |
| <b>Description</b>              | Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.                                                                                                                                                         |
| <b>Options</b>                  | <b>routing-instance routing-instance-name</b> —(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. |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcp server statistics on page 1029</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                 |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                      |

## clear dhcpv6 server binding (Local Server)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>clear dhcpv6 server binding &lt;all   <i>client-id</i>   <i>ip-address</i>   <i>session-id</i>&gt; &lt;interface <i>interface-name</i>&gt; &lt;routing-instance <i>routing-instance-name</i>&gt;</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced in Junos Release 10.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <i>all</i>—(Optional) Clear the binding state for all DHCPv6 clients.</li> <li>• <i>client-id</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).</li> <li>• <i>ip-address</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified address.</li> <li>• <i>session-id</i>—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.</li> <li>• <i>interface interface-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</li> <li>• <i>routing-instance routing-instance-name</i>—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.</li> </ul> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show dhcpv6 server binding (View) on page 1031</a></li> <li>• <i>Junos OS Interfaces Library for Security Devices</i></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## clear dhcpv6 server statistics (Local Server)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear dhcpv6 server statistics</code><br><code>&lt;logical-system <i>logical-system-name</i>&gt;</code><br><code>&lt;routing-instance <i>routing-instance-name</i>&gt;</code>                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos Release 10.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Clear all DHCPv6 local server statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b>logical-system <i>logical-system-name</i></b>—(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><b>routing-instance <i>routing-instance-name</i></b>—(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> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show dhcpv6 server statistics (View) on page 1035</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                  |



---

## clear system login logout

---

|                                 |                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear system login logout<br><all><br><username>                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                   |
| <b>Description</b>              | Unlock the user account locked as a result of invalid login attempts.                                                                                             |
| <b>Options</b>                  | <all>—Clear all locked user accounts.<br><br><username>—Clear the specified locked user account.                                                                  |
| <b>Required Privilege Level</b> | clear                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show system login logout on page 301</a></li><li>• <i>Administration Guide for Security Devices</i></li></ul> |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                  |

## file archive

|                                 |                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file archive destination <i>destination</i> source <i>source</i> &lt;compress&gt;</code>                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>destination <i>destination</i></b>—Name of the created archive. Specify the destination as a URL or filename.</p> <p><b>source <i>source</i></b>— Path of directory to archive.</p> <p><b>compress</b>—(Optional) Compress the archived file with the GNU zip (gzip) compression utility. The compressed files have the suffix <b>.tgz</b>.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <p><a href="#">file archive (Multiple Files) on page 960</a></p> <p><a href="#">file archive (Single File) on page 960</a></p> <p><a href="#">file archive (with Compression) on page 960</a></p>                                                                                                                                                     |
| <b>Output Fields</b>            | 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

---

|                                 |                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file checksum md5 <i>path</i></code>                                                                                                                                                                              |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                         |
| <b>Description</b>              | Calculate the Message Digest 5 (MD5) checksum of a file.                                                                                                                                                                |
| <b>Options</b>                  | <i>path</i> —(Optional) Path to a filename.                                                                                                                                                                             |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <a href="#">file checksum sha1 on page 963</a></li><li>• <a href="#">file checksum sha-256 on page 964</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">file checksum md5 on page 962</a>                                                                                                                                                                           |
| <b>Output Fields</b>            | 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

---

|                                 |                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file checksum sha1 <i>path</i></code>                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5.                                                                                                                                                                            |
| <b>Description</b>              | Calculate the Secure Hash Algorithm (SHA-1) checksum of a file.                                                                                                                                                        |
| <b>Options</b>                  | <i>path</i> —(Optional) Path to a filename.                                                                                                                                                                            |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <a href="#">file checksum md5 on page 962</a></li><li>• <a href="#">file checksum sha-256 on page 964</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">file checksum sha1 on page 963</a>                                                                                                                                                                         |
| <b>Output Fields</b>            | 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/opscrip.sh
```

```
SHA1 (/var/db/scripts/commitscript.sh) = ba9e47120c7ce55c7f29afd73eacd370e162c676
```

## file checksum sha-256

---

|                                 |                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file checksum sha-256 <i>path</i></code>                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5.                                                                                                                                                                         |
| <b>Description</b>              | Calculate the Secure Hash Algorithm 2 family (SHA-256) checksum of a file.                                                                                                                                          |
| <b>Options</b>                  | <i>path</i> —(Optional) Path to a filename.                                                                                                                                                                         |
| <b>Required Privilege Level</b> | maintenance<br>view<br>view-configuration                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <a href="#">file checksum sha1 on page 963</a></li><li>• <a href="#">file checksum md5 on page 962</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">file checksum sha-256 on page 964</a>                                                                                                                                                                   |
| <b>Output Fields</b>            | 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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file compare (files <i>from-file to-file</i>) &lt;context   unified&gt; &lt;ignore-white-space&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | <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"> <li>• <b>default</b>—In the first line of output, <b>c</b> means lines were changed between the two files, <b>d</b> means lines were deleted between the two files, and <b>a</b> 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 (&lt;) in front of output lines refers to the first file. A right angle bracket (&gt;) in front of output lines refers to the second file.</li> <li>• <b>context</b>—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 (-).</li> <li>• <b>unified</b>—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.</li> </ul> |
| <b>Options</b>                  | <p><b>files <i>from-file</i></b>—Names of files to compare.</p> <p><b>files <i>to-file</i></b>—Names of files to compare against.</p> <p><b>context</b>—(Optional) Display output in context format.</p> <p><b>ignore-white-space</b>—(Optional) Ignore changes in the amount of white space.</p> <p><b>unified</b>—(Optional) Display output in unified format.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <p><a href="#">file compare files on page 966</a></p> <p><a href="#">file compare files context on page 966</a></p> <p><a href="#">file compare files unified on page 966</a></p> <p><a href="#">file compare files unified ignore-white-space on page 966</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | 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

|                            |                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>file copy <i>source destination</i></code><br><code>&lt;source-address <i>source- address</i>&gt;</code>                                  |
| <b>Release Information</b> | Command introduced before Junos OS Release 7.4.                                                                                                 |
| <b>Description</b>         | 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>.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                           |
| <b>List of Sample Output</b>    | <a href="#">Copy a File from the Local Device to a Personal Computer on page 968</a><br><a href="#">Copy a Configuration File Between Routing Engines on page 969</a><br><a href="#">Copy a Log File Between Routing Engines on page 969</a><br><a href="#">Copy a File Using FTP on page 969</a><br><a href="#">Copy a File Using FTP and Requiring a Password on page 969</a><br><a href="#">Copy a File Using Secure Copy on page 969</a> |

## 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:/exampleo/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/example.conf re1:/var/tmp/copied-example.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/example.conf` is the local file and `hostname` is the FTP server:

```
user@host> file copy /config/example.conf ftp://hostname/example.conf
Receiving ftp: //hostname/example.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/example.conf` is the local file and `hostname` is the FTP server:

```
root@host> file copy /config/example.conf ftp://user@hostname/example.conf
Password for user@hostname: *****
Receiving ftp: //user@hostname/example.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/example.conf` is the local file, `user` is the username, and `ssh-host` is the scp server:

```
root@host> file copy /config/example.conf scp://user@ssh-host/tmp/example.conf
user@ssh-host's password: *****
example.conf          100%
| ***** |
2198          00:00
```

## file delete

---

|                                 |                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file delete path</code><br><code>&lt;purge&gt;</code>                                                        |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                    |
| <b>Description</b>              | Delete a path on the device.                                                                                       |
| <b>Options</b>                  | <b>path</b> —Name of the path to delete.<br><b>purge</b> —(Optional) Overwrite regular files before deleting them. |
| <b>Required Privilege Level</b> | maintenance                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                 |
| <b>List of Sample Output</b>    | <a href="#">file delete on page 970</a>                                                                            |
| <b>Output Fields</b>            | 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

---

|                                 |                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file list path</code><br><detail   recursive>                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Display a list of paths on the device.                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>path</b>—(Optional) Display a list of paths.</p> <p><b>detail   recursive</b>—(Optional) Display detailed output or descend recursively through the directory hierarchy, respectively.</p>                                                                                                                                                   |
| <b>Additional Information</b>   | 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 <b>file list</b> command. To view files within a specific directory, include a slash followed by the directory and, optionally, subdirectory name after the <b>file list</b> command. |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <a href="#">file list on page 971</a>                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | 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

---

|                                 |                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file rename <i>source destination</i></code>                                                 |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                    |
| <b>Description</b>              | Rename a file on the device.                                                                       |
| <b>Options</b>                  | <i>destination</i> —New name for the file.<br><i>source</i> —Original name of the file.            |
| <b>Required Privilege Level</b> | maintenance                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">file rename on page 972</a>                                                            |
| <b>Output Fields</b>            | 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

|                                 |                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>file show <i>filename</i></code><br><code>&lt;encoding (base64   raw)&gt;</code>                                                                     |
| <b>Release Information</b>      | Command introduced before Junos OS Release 7.4.                                                                                                            |
| <b>Description</b>              | Display the contents of a file.                                                                                                                            |
| <b>Options</b>                  | <p><b><i>filename</i></b>—Name of a file.</p> <p><b>encoding (base64   raw)</b>—(Optional) Encode file contents with base64 encoding or show raw text.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                       |
| <b>List of Sample Output</b>    | <a href="#">file show on page 973</a>                                                                                                                      |
| <b>Output Fields</b>            | 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

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request dhcp client renew</code><br><code>[all interface &lt;interface-name&gt;]</code><br><code>routing-instance &lt;routing-instance-name&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Initiates a renew request for the specified clients if they are in the bound state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b>all</b>—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><b>interface &lt;interface-name&gt;</b>—Initiate renew requests for DHCP clients on the specified interface.</p> <p><b>routing-instance &lt;routing-instance-name&gt;</b>—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> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |




---

## request dhcpv6 client renew

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request dhcpv6 client renew</code><br><code>[all   interface <i>interface-name</i>]</code><br><code>routing-instance &lt;<i>routing-instance-name</i>&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Initiate a renew request for the specified DHCPv6 clients if they are in the bound state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b>all</b>—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><b>interface-name <i>interface-name</i></b>—Initiate renew requests for DHCPv6 clients on the specified interface.</p> <p><b>routing-instance <i>routing-instance-name</i></b>—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> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## request system autorecovery state

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system autorecovery state (save   recover   clear)                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced in Junos Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | Prepares the system for autorecovery of configuration, licenses, and disk information.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>save</b>—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><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.</li> <li>A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.</li> </ul> </div>                        |
|                                 | <p><b>recover</b>—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><b>clear</b>—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>                                                                                                                                                            |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show system autorecovery state on page 292</a></li> <li><i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                  |
| <b>List of Sample Output</b>    | <a href="#">request system autorecovery state save on page 977</a><br><a href="#">request system autorecovery state recover on page 977</a><br><a href="#">request system autorecovery state clear on page 977</a>                                                                                                                                                                                                                                                |
| <b>Output Fields</b>            | 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

---

|                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                    | <code>request system download abort &lt;download-id&gt;</code>                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>                                                                                                                                                       | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>                                                                                                                                                               | 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 <b>show</b> command until a Clear operation is performed.                                                                                                   |
| <div> <b>NOTE:</b> Only downloads in the active, paused, and error states can be aborted.</div> |                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                                                                                                                                                                   | <b>download-id</b> —(Required) The ID number of the download to be paused.                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                  | maintenance                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                                     | <ul style="list-style-type: none"><li>• <a href="#">request system download start on page 279</a></li><li>• <a href="#">request system download pause on page 277</a></li><li>• <a href="#">request system download resume on page 278</a></li><li>• <a href="#">request system download clear on page 276</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul> |
| <b>List of Sample Output</b>                                                                                                                                                     | <a href="#">request system download abort on page 978</a>                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>                                                                                                                                                             | 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

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system download clear                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>              | Delete the history of completed and aborted downloads.                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">request system download start on page 279</a></li><li>• <a href="#">request system download pause on page 277</a></li><li>• <a href="#">request system download resume on page 278</a></li><li>• <a href="#">request system download abort on page 275</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">request system download clear on page 979</a>                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | 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

---


|                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                               | request system download pause <download-id>                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>                                                                                                                                  | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>                                                                                                                                          | Suspend a particular download instance.                                                                                                                                                                                                                                                                                                                                                       |
| <div> <b>NOTE:</b> Only downloads in the active state can be paused.</div> |                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                                                                                                                                              | <b>download-id</b> —(Required) The ID number of the download to be paused.                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                             | maintenance                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                | <ul style="list-style-type: none"><li>• <a href="#">request system download start on page 279</a></li><li>• <a href="#">request system download resume on page 278</a></li><li>• <a href="#">request system download abort on page 275</a></li><li>• <a href="#">request system download clear on page 276</a></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul> |
| <b>List of Sample Output</b>                                                                                                                                | <a href="#">request system download pause on page 980</a>                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>                                                                                                                                        | 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

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                     | <code>request system download resume <i>download-id</i> &lt;max-rate&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>                                                                                                                                                        | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>                                                                                                                                                                | 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 <b>request system download start</b> command. The user can optionally specify a new (maximum) bandwidth with the <b>request system download resume</b> command. |
| <div>  <b>NOTE:</b> Only downloads in the paused and error states can be resumed.         </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                                                                                                                                                                    | <p><b>download-id</b>—(Required) The ID number of the download to be paused.</p> <p><b>max-rate</b>—(Optional) The maximum bandwidth for the download.</p>                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b>                                                                                                                                                   | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>                                                                                                                                                      | <ul style="list-style-type: none"> <li>• <a href="#">request system download start on page 279</a></li> <li>• <a href="#">request system download pause on page 277</a></li> <li>• <a href="#">request system download abort on page 275</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                 |
| <b>List of Sample Output</b>                                                                                                                                                      | <a href="#">request system download resume on page 981</a>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Output Fields</b>                                                                                                                                                              | 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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request system download start (url   max-rate   save as   login   delay)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Creates a new download instance and identifies it with a unique integer called the download ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>url</b>—(Required) The FTP or HTTP URL location of the file to be downloaded.</p> <p><b>max-rate</b>—(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><b>save-as</b>—(Optional) The filename to be used for saving the file in the <code>/var/tmp</code> location.</p> <p><b>login</b>—(Optional) The username and password for the server in the format <code>username:password</code>.</p> <p><b>delay</b>—(Optional) The number of hours after which the download should start.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">request system download pause on page 277</a></li> <li>• <a href="#">request system download resume on page 278</a></li> <li>• <a href="#">request system download abort on page 275</a></li> <li>• <a href="#">request system download clear on page 276</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                    |
| <b>List of Sample Output</b>    | <a href="#">request system download start on page 982</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | 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

|                                 |                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system firmware upgrade                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Release 10.2 of Junos OS.                                                                                                                                                                                      |
| <b>Description</b>              | Upgrade firmware on a system.                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>fpc</b>—Upgrade FPC ROM monitor.</p> <p><b>pic</b>—Upgrade PIC firmware.</p> <p><b>re</b>—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.</p> <p><b>vcpu</b>—Upgrade VCPU ROM monitor.</p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                           |
| <b>List of Sample Output</b>    | <a href="#">request system firmware upgrade on page 983</a>                                                                                                                                                                          |
| <b>Output Fields</b>            | 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 license update

---

|                                 |                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system license update                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5.                                                                                                                                                                                              |
| <b>Description</b>              | Start autoupdating license keys from the LMS server.                                                                                                                                                                                     |
| <b>Options</b>                  | <b>trial</b> —Starts autoupdating trial license keys from the LMS server.                                                                                                                                                                |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Administration Guide for Security Devices</i></li><li>• <i>UTM Overview Feature Guide for Security Devices</i></li><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">request system license update on page 984</a><br><a href="#">request system license update trial on page 984</a>                                                                                                             |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                    |

### Sample Output

#### request system license update

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

```
Request to automatically update license keys from https://ae1.juniper.net has  
been sent, use show system license to check status.
```

#### request system license update trial

```
user@host> request system license update trial
```

```
Request to automatically update trial license keys from https://ae1.juniper.net  
has been sent, use show system license to check status.
```

## request system partition compact-flash

|                                 |                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system partition compact-flash                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Release 9.2 of Junos OS.                                                                                                                                                                                                                                             |
| <b>Description</b>              | Reboots the device and repartitions the compact flash. The compact flash is repartitioned only if it is possible to restore all the data on the compact flash. Otherwise, the operation is aborted, and a message is displayed indicating that the current disk usage needs to be reduced. |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Example: Installing Junos OS on SRX Series Devices Using the Partition Option on page 193</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                        |
| <b>List of Sample Output</b>    | <a href="#">request system partition compact-flash (If Yes) on page 985</a><br><a href="#">request system partition compact-flash (If No) on page 985</a>                                                                                                                                  |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                      |

### Sample Output

#### request system partition compact-flash (If Yes)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] yes
Initiating repartition operation.
The operation may take several minutes to complete.
System will reboot now...
<System reboots>
<Repartition operation is performed>
<System reboots and starts up normally>

```

### Sample Output

#### request system partition compact-flash (If No)

```

user@host> request system partition compact-flash
Are you sure you want to reboot
and partition the compact-flash ? [yes,no] no

```

## request system power-off fpc

---

|                                 |                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system (halt   power-off   reboot) power-off fpc                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.4.                                                                                                                                                                                                                |
| <b>Description</b>              | Bring Flexible PIC Concentrators (FPCs) offline before Routing Engines are shut down.                                                                                                                                                                       |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b>halt</b>—Bring FPC offline and then halt the system.</li><li>• <b>power-off</b>—Bring FPC offline and then power off the system.</li><li>• <b>reboot</b>—Bring FPC offline and then reboot the system.</li></ul> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li></ul>                                                                                                                                                |
| <b>List of Sample Output</b>    | <a href="#">request system halt power-off fpc on page 986</a><br><a href="#">request system power-off power-off fpc on page 986</a><br><a href="#">request system reboot power-off fpc on page 986</a>                                                      |
| <b>Output Fields</b>            | 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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request system services dhcp (release <i>interface-name</i>   renew <i>interface-name</i>)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Release 8.5 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <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 <b>show system services dhcp client <i>interface-name</i></b> command.</p>                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>release <i>interface-name</i></b> —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.</li> <li>• <b>renew <i>interface-name</i></b> —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.</li> </ul> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>dhcp</i></li> <li>• <a href="#">show system services dhcp client on page 124</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>    | <a href="#">request system services dhcp client release ge-1/0/1 on page 987</a><br><a href="#">request system services dhcp client renew ge-1/0/1 on page 987</a>                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | 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 Release 10.2 of Junos OS.

**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 193](#)
- *Installation and Upgrade Guide for Security Devices*

**List of Sample Output**

[request system snapshot media hard-disk on page 989](#)  
[request system snapshot media usb \(when usb device is missing on page 989](#)  
[request system snapshot media compact-flash on page 990](#)  
[request system snapshot media internal on page 990](#)  
[request system snapshot partition on page 990](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### [request system snapshot media hard-disk](#)

```
user@host> request system snapshot media hard-disk
Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...
```

### [request system snapshot media usb \(when usb device is missing](#)

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

```
Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
```

#### request system snapshot media compact-flash

```
user@host> request system snapshot media compact-flash
error: cannot snapshot to current boot device
```

#### request system snapshot 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)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system software abort in-service-upgrade                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | 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 <b>request system in-service-upgrade</b> 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. |
| <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>request system software in-service-upgrade (Maintenance)</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">request system software abort in-service-upgrade on page 991</a>                                                                                                                                                                                                                                                                                                                                    |
| <b>Output Fields</b>            | 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)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request system software add <i>package-name</i></code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Partition option introduced in the command in Release 10.1. of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Installs the new software package on the device. For example: <b>request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <code>delay-restart</code> — Installs the software package but does not restart the software process</li><li>• <code>best-effort-load</code> — Activate a partial load and treat parsing errors as warnings instead of errors</li><li>• <code>no-copy</code> — Installs the software package but does not saves the copies of package files</li><li>• <code>no-validate</code> — Does not check the compatibility with current configuration before installation starts</li><li>• <code>partition</code> — Formats and re-partitions the media before installation</li><li>• <code>reboot</code> — Reboots the device after installation is completed</li><li>• <code>unlink</code> — Removes the software package after successful installation</li><li>• <code>validate</code> — Checks the compatibility with current configuration before installation starts</li></ul> |
| <b>Required Privilege Level</b> | <code>maintenance</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## request system reboot

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>request system reboot &lt;at time&gt; &lt;in minutes&gt;&lt;media&gt;&lt;message 'text'&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Reboots the software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <i>at time</i>— 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"> <li>• <i>now</i>— Reboots the device immediately. This is the default.</li> <li>• <i>+minutes</i>— Reboots the device in the number of minutes from now that you specify.</li> <li>• <i>yymmddhhmm</i>— Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.</li> <li>• <i>hh:mm</i>— 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.</li> </ul> </li> <li>• <i>in minutes</i>— Specifies the number of minutes from now to reboot the device. This option is a synonym for the <i>at +minutes</i> option</li> <li>• <i>media type</i>— Specifies the boot device to boot the device from: <ul style="list-style-type: none"> <li>• <i>disk/internal</i>— Reboots from the internal media. This is the default.</li> <li>• <i>usb</i>— Reboots from the USB storage device.</li> <li>• <i>compact flash</i>— Reboots from the external compact flash. This option is available on the SRX650 Services Gateway.</li> </ul> </li> <li>• <i>message text</i>— Provides a message to display to all system users before the device reboots.</li> </ul> <p>Example: <b>request system reboot at 5 in 50 media internal message stop</b></p> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">request system software rollback (Maintenance) on page 290</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## request system software rollback (Maintenance)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | request system software rollback<br><node <i>node-id</i> >   <all>   <local>   <primary><br><reboot>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.1.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Revert to the software that was loaded at the last successful <b>request system software add</b> command. Example: <b>request system software rollback</b> .                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <ul style="list-style-type: none"><li>• <b>node <i>node-id</i></b>—(High-end SRX Series devices only) Roll back the software to the previous set of packages on a specific node.</li><li>• <b>all</b>— Roll back the software on all the nodes.</li><li>• <b>local</b>— Roll back the software on the local node.</li><li>• <b>primary</b>— Roll back the software on the primary node.</li><li>• <b>reboot</b>— Reboot the system after a roll back.</li></ul> |
| <b>Required Privilege Level</b> | maintenance                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Installation and Upgrade Guide for Security Devices</i></li><li>• <i>Administration Guide for Security Devices</i></li></ul>                                                                                                                                                                                                                                                                                         |

## request support information

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>List of Syntax</b>                                 | <a href="#">Syntax on page 995</a><br><a href="#">Syntax (SRX Series) on page 995</a><br><a href="#">Syntax (EX Series Switch and MX Series Router) on page 995</a><br><a href="#">Syntax (TX Matrix Router) on page 995</a><br><a href="#">Syntax (TX Matrix Plus Router) on page 995</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Syntax</b>                                         | request support information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Syntax (SRX Series)</b>                            | request support information<br><node ( <i>node id</i>   all   local   primary)>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Syntax (EX Series Switch and MX Series Router)</b> | request support information<br><all-members><br><local><br><member <i>member-id</i> >                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Syntax (TX Matrix Router)</b>                      | request support information<br><all-lcc   lcc <i>number</i>   scc>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Syntax (TX Matrix Plus Router)</b>                 | request support information<br><all-chassis   all-lcc   lcc <i>number</i>   sfc <i>number</i> >                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>                            | Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>                                    | Display information about 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 <b>show</b> commands, with the appropriate information for your device automatically included.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                                        | <p><b>node</b><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><b>all</b>—(SRX Series) (Optional) Display system information for all nodes.</p> <p><b>local</b>—(SRX Series) (Optional) Display system information for local node.</p> <p><b>primary</b>—(SRX Series) (Optional) Display system information for primary node.</p> <p><b>all-chassis</b>—(TX Matrix and TX Matrix Plus routers) (Optional) Display system information for all chassis.</p> <p><b>all-lcc</b>—(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 996](#) 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        |

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.

**Required Privilege Level** maintenance

**Related Documentation**

- [Request Support Information Overview](#)

**List of Sample Output**

[request support information | save on page 997](#)  
[request support information scc \(TX Matrix Router\) on page 997](#)  
[request support information sfc \(TX Matrix Plus Router\) on page 998](#)  
[request support information \(SRX Series\) on page 1001](#)

**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
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
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    OK    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    OK    12K      0:18  0.00% bcmLINK.0
   1345 root      1   76   0    OK    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: 2015-06-11 20:55:12 UTC
System booted: 2015-06-11 17:45:22 UTC (03:09:50 ago)
Protocols started: 2015-06-11 17:47:59 UTC (03:07:13 ago)
Last configured: 2015-04-27 17:41:45 UTC (6w3d 03:13 ago) by root
8:55PM up 3:10, 2 users, load averages: 0.09, 0.06, 0.01

user@host> show version detail no-forwarding

Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.1-20150403_dev_x_121_x46.2]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.1-20150403_dev_x_121_x46.2 #0 built by builder on 2015-04-04 00:06:53
UTC
MGD release 12.1D0.2 built by builder on 2015-04-04 01:59:04 UTC
CLI release 12.1-20150403_dev_x_121_x46.2 built by builder on 2015-04-04 00:18:42
UTC
RPD release 12.1D0.2 built by builder on 2015-04-04 01:48:23 UTC
...

user@host> request support information node all
node0:
-----

user@host> show system uptime

node0:
-----
Current time: 2015-06-11 20:57:06 UTC
System booted: 2015-06-11 17:45:22 UTC (03:11:44 ago)
Protocols started: 2015-06-11 17:47:59 UTC (03:09:07 ago)
Last configured: 2015-04-27 17:41:45 UTC (6w3d 03:15 ago) by root
8:57PM up 3:12, 2 users, load averages: 0.04, 0.05, 0.01

user@host> show version detail no-forwarding

Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.1-20150403_dev_x_121_x46.2]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]

```

```
KERNEL 12.1-20150403_dev_x_121_x46.2 #0 built by builder on 2015-04-04 00:06:53
UTC
MGD release 12.1D0.2 built by builder on 2015-04-04 01:59:04 UTC
CLI release 12.1-20150403_dev_x_121_x46.2 built by builder on 2015-04-04 00:18:42
UTC
RPD release 12.1D0.2 built by builder on 2015-04-04 01:48:23 UTC
...
```

```
user@host> request support information node local
node0:
```

```
user@host> show system uptime
```

```
node0:
```

```
-----
Current time: 2015-06-11 20:57:55 UTC
System booted: 2015-06-11 17:45:22 UTC (03:12:33 ago)
Protocols started: 2015-06-11 17:47:59 UTC (03:09:56 ago)
Last configured: 2015-04-27 17:41:45 UTC (6w3d 03:16 ago) by root
8:57PM up 3:13, 2 users, load averages: 0.02, 0.04, 0.00
```

```
user@host> show version detail no-forwarding
```

```
Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.1-20150403_dev_x_121_x46.2]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.1-20150403_dev_x_121_x46.2 #0 built by builder on 2015-04-04 00:06:53
UTC
MGD release 12.1D0.2 built by builder on 2015-04-04 01:59:04 UTC
CLI release 12.1-20150403_dev_x_121_x46.2 built by builder on 2015-04-04 00:18:42
UTC
RPD release 12.1D0.2 built by builder on 2015-04-04 01:48:23 UTC
...
```

```
user@host> request support information node primary
node0:
```

```
user@host> show system uptime
```

```
node0:
```

```
-----
Current time: 2015-06-11 20:58:35 UTC
System booted: 2015-06-11 17:45:22 UTC (03:13:13 ago)
Protocols started: 2015-06-11 17:47:59 UTC (03:10:36 ago)
Last configured: 2015-04-27 17:41:45 UTC (6w3d 03:16 ago) by root
8:58PM up 3:13, 2 users, load averages: 0.28, 0.11, 0.03
```

```
user@host> show version detail no-forwarding
```

```
Hostname: tpsrx02
Model: srx1400
JUNOS Software Release [12.1-20150403_dev_x_121_x46.2]
JUNOS wmi Daemon [12.1I20140304_0803_tjzhang]
KERNEL 12.1-20150403_dev_x_121_x46.2 #0 built by builder on 2015-04-04 00:06:53
UTC
MGD release 12.1D0.2 built by builder on 2015-04-04 01:59:04 UTC
```

```
CLI release 12.1-20150403_dev_x_121_x46.2 built by builder on 2015-04-04 00:18:42
UTC
RPD release 12.1D0.2 built by builder on 2015-04-04 01:48:23 UTC
...
```

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 reboot on page 289](#)
- [request system software rollback \(Maintenance\) on page 290](#)

**List of Sample Output** [request system zeroize on page 1004](#)

### 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)

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>List of Syntax</b>               | <a href="#">Syntax (High-end SRX Series) on page 1006</a><br><a href="#">Syntax (Branch SRX Series) on page 1006</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Syntax (High-end SRX Series)</b> | <pre>restart &lt;application-identification  application-security  audit-process  chassis-control  class-of-service  database-replication  datapath-trace-service  ddns  dhcp  dhcp-service  disk-monitoring  dynamic-flow-capture  ethernet-connectivity-fault-management  ethernet-link-fault-management  event-processing  fipsd  firewall  firewall-authentication-service  general-authentication-service  gprs-process  gracefully  idp-policy  immediately  interface-control  ipmi  ipsec-key-management  jnx-wmi-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  pki-service  profilerd  remote-operations  routing  sampling  secure-neighbor-discovery  security-intelligence  security-log  service-deployment  simple-mail-client-service  snmp  soft  statistics-service  subscriber-management  subscriber-management-helper  tunnel-oamd  uac-service  vrrp  web-management&gt;</pre>                                                                                                                                                                  |
| <b>Syntax (Branch SRX Series)</b>   | <pre>restart &lt; 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  ethernet-connectivity-fault-management  ethernet-link-fault-management  ethernet-switching  event-processing  firewall  firewall-authentication-service  forwarding  general-authentication-service  gracefully  group-key-member  group-key-server  idp-policy  immediately  interface-control  ipmi  ipsec-key-management  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  peer-selection-service  pgm  pki-service  ppp  pppoe  profilerd  r2cp  remote-operations  routing  sampling  sdk-service  secure-neighbor-discovery  security-intelligence  security-log  service-deployment  services  simple-mail-client-service  snmp  soft  statistics-service  subscriber-management  subscriber-management-helper  system-health-management  uac-service  usb-control  vrrp  web-management  wireless-lan-service  wireless-wan-service&gt;</pre> |
| <b>Release Information</b>          | <p>Command introduced before Junos OS Release 7.4.</p> <p><b>dynamic-flow-capture</b> option added in Junos OS Release 7.4.</p> <p><b>event-processing</b> option added in Junos OS Release 7.5.</p> <p><b>group-key-server</b> option added in Junos OS Release 10.2.</p> <p><b>ppp</b> option added in Junos OS Release 7.5.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>                  | 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-services—(Branch SRX Series only) (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.
- **jnx-wmi-service**—(High-end SRX Series only) (Optional) Restart the jnx Windows Management Instrumentation (WMI) 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—(High-end SRX Series only) (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.

- `profillerd`—(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 (`rpd`).
- `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.
- `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.
- `usb-control`—(Branch SRX Series only) (Optional) Restart the USB control process.
- `vrrp`—(Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that

LAN without requiring more than the static configuration of a single default route on the hosts.

- web-management—(Optional) Restart the Web management process.
- 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**

- *Administration Guide for Security Devices*
- [Restart Commands Overview on page 1011](#)

**List of Sample Output**    [restart interfaces on page 1011](#)

**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*
- *Administration Guide for Security Devices*

## show chassis routing-engine (View)

|                                 |                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show chassis routing-engine                                                                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5.                                                                                                                                |
| <b>Description</b>              | Display the Routing Engine status of the chassis cluster.                                                                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                         |
| <b>List of Sample Output</b>    | <a href="#">show chassis routing-engine on page 1013</a><br><a href="#">show chassis routing-engine on page 1013</a>                                                       |
| <b>Output Fields</b>            | Table 103 on page 1012 lists the output fields for the <b>show chassis routing-engine</b> 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.                                                   |
| CPU temperature      | CPU temperature.                                                              |
| 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.                                                    |
| Uptime               | Length of time the Routing Engine has been up (running) since the last start. |

Table 103: show chassis routing-engine Output Fields (*continued*)

| Field Name         | Field Description                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| 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

```

user@host> show chassis routing-engine (Sample 1)
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

```

user@host> show chassis routing-engine (Sample 2)
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

```

## show dhcp client binding

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcp client binding<br>[<address>   interface <interface-name>]<br>routing-instance <routing-instance name><br>[brief   detail   summary ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>address</b>—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:</p> <ul style="list-style-type: none"> <li>ip-address—The specified IP address.</li> <li>mac-address—The specified MAC address.</li> </ul> <p><b>routing-instance &lt;routing-instance name&gt;</b>—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.</p> <p><b>interface &lt;interface-name&gt;</b>—(Optional) Perform this operation on the specified interface.</p> <p><b>brief</b>—(Optional) Display brief information about the active client bindings.</p> <p><b>detail</b>—(Optional) Display detailed client binding information.</p> <p><b>summary</b>—(Optional) Display a summary of DHCP client information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear dhcp client binding on page 949</a></li> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>List of Sample Output</b>    | <a href="#">show dhcp client binding on page 1015</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | Table 104 on page 1014 lists the output fields for the <b>show dhcp client binding</b> 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.       |



Table 104: show dhcp client binding Output Fields (*continued*)

| Field Name        | Field Description                                             |
|-------------------|---------------------------------------------------------------|
| Expires           | Number of seconds in which the lease expires.                 |
| 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<br>fe-0/0/1.0 | 00:0a:12:00:12:12 |        | 10.1.1.1 | 348   | BOUND     |

## show dhcpv6 client binding

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcpv6 client binding<br>interface <i>interface-name</i><br>routing-instance < <i>routing-instance-name</i> ><br>[brief   detail   summary]                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>interface <i>interface-name</i></b>—(Optional) Perform this operation on the specified interface.</p> <p><b>routing-instance <i>routing-instance-name</i></b>—(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.</p> <p><b>brief</b>—(Optional) Display brief information about the active client bindings.</p> <p><b>detail</b>—(Optional) Display detailed client binding information.</p> <p><b>summary</b>—(Optional) Display a summary of DHCPv6 client information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcpv6 client binding on page 950</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 client binding on page 1018</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Output Fields</b>            | Table 105 on page 1017 lists the output fields for the <b>show dhcpv6 client binding</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                            |

Table 105: 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 105: 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 statefull. |
| 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          STATEFULL  BOUND      ge-0/0/1.0
LL_TIME0x3-0x0-2c:6b:f5:62:39:c1

```

### show dhcpv6 client binding detail

```

user@host> 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            VEND0R0x00000583-0x3000103f
  Bind Type:             IA_NA
  ClientType :           STATEFULL
  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 dhcp client statistics

|                                 |                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcp client statistics<br>routing-instance <routing-instance-name>                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                      |
| <b>Description</b>              | Display Dynamic Host Configuration Protocol (DHCP) client statistics.                                                                                                      |
| <b>Options</b>                  | <b>routing-instance routing-instance-name</b> —(Optional) Display the statistics for DHCP clients on the specified routing instance.                                       |
| <b>Required Privilege Level</b> | view                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp client statistics on page 951</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>   |
| <b>List of Sample Output</b>    | <a href="#">show dhcp client statistics on page 1020</a>                                                                                                                   |
| <b>Output Fields</b>            | Table 106 on page 1019 lists the output fields for the <b>show dhcp client statistics</b> command. Output fields are listed in the approximate order in which they appear. |

Table 106: 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"> <li>• BOOTREPLY—Number of BOOTP protocol data units (PDUs) received</li> <li>• DHCPOFFER—Number of DHCP PDUs of type OFFER received</li> <li>• DHCPACK—Number of DHCP PDUs of type ACK received</li> <li>• DHCPNACK—Number of DHCP PDUs of type NACK received</li> <li>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received</li> </ul> |

Table 106: show dhcp client statistics (*continued*)

| Field Name    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Messages sent | <p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> <li>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted</li> <li>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted</li> <li>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted</li> <li>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted</li> <li>• DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted</li> <li>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted</li> <li>• DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted</li> <li>• DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted</li> </ul> |

## 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 dhcpv6 client statistics

|                                 |                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcpv6 client statistics<br>routing-instance<routing-instance-name>                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X45-D10.                                                                                                                        |
| <b>Description</b>              | Display Dynamic Host Configuration Protocol (DHCPv6) client statistics.                                                                                                      |
| <b>Options</b>                  | <b>routing-instance &lt;routing-instance-name&gt;</b> —(Optional) Display the statistics for DHCPv6 clients on the specified routing instance.                               |
| <b>Required Privilege Level</b> | view                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcpv6 client statistics on page 952</a></li> </ul>                                                               |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 client statistics on page 1022</a>                                                                                                                   |
| <b>Output Fields</b>            | Table 107 on page 1021 lists the output fields for the <b>show dhcpv6 client statistics</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 107: 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"> <li>• DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE transmitted</li> <li>• DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT transmitted</li> <li>• DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted</li> <li>• DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE transmitted</li> <li>• DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST transmitted</li> <li>• DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM transmitted</li> <li>• DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW transmitted</li> <li>• DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND transmitted</li> </ul> |

Table 107: 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"> <li>DHCPV6_ADVERTISE—Number of DHCPv6 PDUs of type ADVERTISE received</li> <li>DHCPV6_REPLY—Number of DHCPv6 PDUs of type REPLY received</li> <li>DHCPV6_RECONFIGURE—Number of DHCPv6 PDUs of type RECONFIGURE received</li> </ul> |

## 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 dhcp relay binding

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | Show dhcp relay binding<br>[<address>   interface <interface-name>]<br>routing-instance <routing-instance name><br>[brief   detail   summary]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                  | <p><b>address</b>—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:</p> <ul style="list-style-type: none"> <li>ip-address—The specified IP address.</li> <li>mac-address—The specified MAC address.</li> </ul> <p><b>routing-instance &lt;routing-instance name&gt;</b>—(Optional) Display DHCP binding information on the specified routing instance.</p> <p><b>interface &lt;interface-name&gt;</b>—(Optional) Perform this operation on the specified interface.</p> <p><b>brief</b>—(Optional) Display brief information about the active client bindings.</p> <p><b>detail</b>—(Optional) Display detailed client binding information.</p> <p><b>summary</b>—(Optional) Display a summary of DHCP client information.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear dhcp relay binding on page 953</a></li> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>List of Sample Output</b>    | <a href="#">show dhcp relay binding on page 1024</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Output Fields</b>            | Table 108 on page 1023 lists the output fields for the <b>show dhcp relay binding</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 108: 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. |

Table 108: show dhcp relay binding Output Fields (*continued*)

| Field Name  | Field Description                                             |
|-------------|---------------------------------------------------------------|
| Type        | Type of DHCP packet processing performed on the device.       |
| 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

|                                 |                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcp relay statistics<br>[<routing-instance>]                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                     |
| <b>Description</b>              | Display Dynamic Host Configuration Protocol (DHCP) relay statistics.                                                                                                      |
| <b>Options</b>                  | <b>routing-instance</b> —(Optional) Display the DHCP relay statistics on the specified routing instance.                                                                  |
| <b>Required Privilege Level</b> | view                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp relay statistics on page 954</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>   |
| <b>List of Sample Output</b>    | <a href="#">show dhcp relay statistics on page 1025</a>                                                                                                                   |
| <b>Output Fields</b>            | Table 109 on page 1025 lists the output fields for the <b>show dhcp relay statistics</b> command. Output fields are listed in the approximate order in which they appear. |

Table 109: show dhcp relay statistics

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Messages received | <p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> <li>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received</li> <li>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE received</li> <li>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received</li> <li>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST received</li> <li>• DHCPINFORM—Number of DHCP PDUs of type INFORM received</li> <li>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE received</li> </ul> |
| Messages sent     | <p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> <li>• BOOTREPLY—Number of BOOTP PDUs transmitted</li> <li>• DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted</li> <li>• DHCPACK—Number of DHCP PDUs of type ACK transmitted</li> <li>• DHCPNACK—Number of DHCP PDUs of type NACK transmitted</li> <li>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted</li> </ul>                                                                                      |

## 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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcp server binding<br>[interface <interface name>]<br><brief   detail   summary   verbose><br><ip-address   MAC address><br><routing-instance routing-instance-name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>interface &lt;interface name&gt;</b>—(Optional) Display information about active client bindings on the specified interface.</p> <p><b>brief   detail   summary</b>—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as <b>show dhcp server binding</b>.</p> <p><b>ip-address</b>—Display DHCP binding information for a specific client identified by the specified IP address.</p> <p><b>MAC address</b>—Display DHCP binding information for a specific client identified by the specified MAC address.</p> <p><b>routing-instance routing-instance-name</b>—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp server binding on page 955</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show dhcp server binding on page 1028</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | <a href="#">Table 110 on page 1027</a> lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 110: 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. |

Table 110: show dhcp server binding Output Fields (*continued*)

| Field Name  | Field Description                                             |
|-------------|---------------------------------------------------------------|
| Type        | Type of DHCP packet processing performed on the device.       |
| 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

|                                 |                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcp server statistics<br><routing-instance>                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1X44-D10.                                                                                                                                                                              |
| <b>Description</b>              | Display d Dynamic Host Configuration Protocol (DHCP) local server statistics.                                                                                                                                                      |
| <b>Options</b>                  | <b>routing-instance</b> —(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. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcp server statistics on page 956</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                           |
| <b>List of Sample Output</b>    | <a href="#">show dhcp server statistics on page 1030</a>                                                                                                                                                                           |
| <b>Output Fields</b>            | Table 111 on page 1029 lists the output fields for the <b>show dhcp server statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                         |

**Table 111: 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"> <li>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received</li> <li>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE received</li> <li>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received</li> <li>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST received</li> <li>• DHCPINFORM—Number of DHCP PDUs of type INFORM received</li> <li>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE received</li> </ul> |
| Messages sent     | Number of DHCP messages received. <ul style="list-style-type: none"> <li>• BOOTREPLY—Number of BOOTP PDUs transmitted</li> <li>• DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted</li> <li>• DHCPACK—Number of DHCP PDUs of type ACK transmitted</li> <li>• DHCPNACK—Number of DHCP PDUs of type NACK transmitted</li> <li>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted</li> </ul>                                                                                      |

## 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 server binding (View)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show dhcpv6 server binding<br><brief   detail   summary><br><interface <i>interface-name</i> ><br><routing-instance <i>routing-instance-name</i> >                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Command introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | Display the address bindings in the client table for DHCPv6 local server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• brief   detail   summary—(Optional) Display the specified level of output about active client bindings. The default is <b>brief</b>, which produces the same output as <b>show dhcpv6 server binding</b>.</li> <li>• interface <i>interface-name</i>—(Optional) Display information about active client bindings on the specified interface.</li> <li>• routing-instance <i>routing-instance-name</i>—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.</li> </ul> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcpv6 server binding (Local Server) on page 957</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 server binding on page 1032</a><br><a href="#">show dhcpv6 server binding detail on page 1033</a><br><a href="#">show dhcpv6 server binding interface on page 1033</a><br><a href="#">show dhcpv6 server binding interface detail on page 1033</a><br><a href="#">show dhcpv6 server binding prefix on page 1034</a><br><a href="#">show dhcpv6 server binding session-id on page 1034</a><br><a href="#">show dhcpv6 server binding summary on page 1034</a>                                                                                       |
| <b>Output Fields</b>            | Table 112 on page 1031 lists the output fields for the <b>show dhcpv6 server binding</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 112: show dhcpv6p server binding Output Fields

| Field Name                                                                                                                                                                              | Field Description                                                                                    | Level of Output |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------|
| <i>number</i> clients,<br>( <i>number</i> init,<br><i>number</i> bound,<br><i>number</i> selecting,<br><i>number</i> requesting,<br><i>number</i> renewing,<br><i>number</i> releasing) | Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state. | <b>summary</b>  |

Table 112: show dhc6p server binding Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Level of Output               |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <b>Prefix</b>                    | Client's DHCPv6 prefix.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>brief</b><br><b>detail</b> |
| <b>Session Id</b>                | Session ID of the subscriber session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>brief</b><br><b>detail</b> |
| <b>Expires</b>                   | Number of seconds in which lease expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>brief</b><br><b>detail</b> |
| <b>State</b>                     | State of the address binding table on the DHCPv6 local server: <ul style="list-style-type: none"> <li>• <b>BOUND</b>—Client has active IP address lease.</li> <li>• <b>INIT</b>—Initial state.</li> <li>• <b>RELEASE</b>—Client is releasing IP address lease.</li> <li>• <b>RECONFIGURE</b>—Client has received reconfigure message from server.</li> <li>• <b>RENEWING</b>—Client sending request to renew IP address lease.</li> <li>• <b>REQUESTING</b>—Client requesting a DHCPv6 server.</li> <li>• <b>SELECTING</b>—Client receiving offers from DHCPv6 servers.</li> </ul> | <b>brief</b><br><b>detail</b> |
| <b>Interface</b>                 | Interface on which the DHCPv6 request was received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>brief</b>                  |
| <b>Client DUID</b>               | Client's DHCP Unique Identifier (DUID).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>brief</b><br><b>detail</b> |
| <b>Lease expires</b>             | Date and time at which the client's IP address lease expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>detail</b>                 |
| <b>Lease expires in</b>          | Number of seconds in which lease expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>                 |
| <b>Lease Start</b>               | Date and time at which the client's address lease was obtained.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>detail</b>                 |
| <b>Incoming Client Interface</b> | Client's incoming interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>detail</b>                 |
| <b>Server IP Address</b>         | IP address of DHCPv6 server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>detail</b>                 |
| <b>Server Interface</b>          | Interface of DHCPv6 server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>detail</b>                 |
| <b>Client Id length</b>          | Length of the DHCPv6 client ID, in bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>detail</b>                 |
| <b>Client Id</b>                 | ID of the DHCPv6 client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>detail</b>                 |

## 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  | LL_TIME0x1-0x2e159c0-00:10:94:00:00:01 | 86321   | BOUND | ge-1/0/0.0 |             |
| 2001:bd8:1111:2222::/64 7  | LL_TIME0x1-0x2e159c0-00:10:94:00:00:02 | 86321   | BOUND | ge-1/0/0.0 |             |
| 2001:bd8:1111:2222::/64 8  | LL_TIME0x1-0x2e159c0-00:10:94:00:00:03 | 86321   | BOUND | ge-1/0/0.0 |             |
| 2001:bd8:1111:2222::/64 9  | LL_TIME0x1-0x2e159c1-00:10:94:00:00:04 | 86321   | BOUND | ge-1/0/0.0 |             |
| 2001:bd8:1111:2222::/64 10 | LL_TIME0x1-0x2e159c1-00:10:94:00:00:05 | 86321   | BOUND | ge-1/0/0.0 |             |

### 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)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dhcpv6 server statistics</b><br><b>&lt;logical-system <i>logical-system-name</i>&gt;</b><br><b>&lt;routing-instance <i>routing-instance-name</i>&gt;</b>                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Release 10.4 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display DHCPv6 local server statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b>logical-system <i>logical-system-name</i></b>—(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><b>routing-instance <i>routing-instance-name</i></b>—(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> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear dhcpv6 server statistics (Local Server) on page 958</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">show dhcpv6 server statistics on page 1037</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 113 on page 1036</a> lists the output fields for the <b>show dhcpv6 server statistics</b> 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dhcpv6 Packets dropped</b> | <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"> <li>• <b>Total</b>—Total number of packets discarded by the DHCPv6 local server</li> <li>• <b>Strict Reconfigure</b>—Number of solicit messages discarded because the client does not support reconfiguration</li> <li>• <b>Bad hardware address</b>—Number of packets discarded because an invalid hardware address was specified</li> <li>• <b>Bad opcode</b>—Number of packets discarded because an invalid operation code was specified</li> <li>• <b>Bad options</b>—Number of packets discarded because invalid options were specified</li> <li>• <b>Invalid server address</b>—Number of packets discarded because an invalid server address was specified</li> <li>• <b>No available addresses</b>—Number of packets discarded because there were no addresses available for assignment</li> <li>• <b>No interface match</b>—Number of packets discarded because they did not belong to a configured interface</li> <li>• <b>No routing instance match</b>—Number of packets discarded because they did not belong to a configured routing instance</li> <li>• <b>No valid local address</b>—Number of packets discarded because there was no valid local address</li> <li>• <b>Packet too short</b>—Number of packets discarded because they were too short</li> <li>• <b>Read error</b>—Number of packets discarded because of a system read error</li> <li>• <b>Send error</b>—Number of packets that the DHCPv6 local server could not send</li> </ul> |
| <b>Messages received</b>      | <p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> <li>• <b>DHCPV6_CONFIRM</b>—Number of DHCPv6 CONFIRM PDUs received.</li> <li>• <b>DHCPV6_DECLINE</b>—Number of DHCPv6 DECLINE PDUs received.</li> <li>• <b>DHCPV6_INFORMATION_REQUEST</b>—Number of DHCPv6 INFORMATION-REQUEST PDUs received.</li> <li>• <b>DHCPV6_REBIND</b>—Number of DHCPv6 REBIND PDUs received.</li> <li>• <b>DHCPV6_RELAY_FORW</b>—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the DHCPv6 server.</li> <li>• <b>DHCPV6_RELEASE</b>—Number of DHCPv6 RELEASE PDUs received.</li> <li>• <b>DHCPV6_RENEW</b>—Number of DHCPv6 RENEW PDUs received.</li> <li>• <b>DHCPV6_REQUEST</b>—Number of DHCPv6 REQUEST PDUs received.</li> <li>• <b>DHCPV6_SOLICIT</b>—Number of DHCPv6 SOLICIT PDUs received.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Messages sent</b>          | <p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> <li>• <b>DHCPV6_ADVERTISE</b>—Number of DHCPv6 ADVERTISE PDUs transmitted.</li> <li>• <b>DHCPV6_REPLY</b>—Number of DHCPv6 ADVERTISE PDUs transmitted.</li> <li>• <b>DHCPV6_RECONFIGURE</b>—Number of DHCPv6 RECONFIGURE PDUs transmitted.</li> <li>• <b>DHCPV6_RELAY_REPL</b>—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 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)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>show firewall &lt;filter <i>filter-name</i>&gt; &lt;counter <i>counter-name</i>&gt; &lt;log&gt; &lt;prefix-action-stats&gt; &lt;terse&gt;</pre>                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Command introduced before Release 10.0 of Junos OS.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Display statistics about configured firewall filters.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                  | <p><b>none</b>—Display statistics about configured firewall filters.</p> <p><b>filter <i>filter-name</i></b>—Name of a configured filter.</p> <p><b>counter <i>counter-name</i></b>—Name of a filter counter.</p> <p><b>log</b>—Display log entries for firewall filters.</p> <p><b>prefix-action-stats</b>—Display prefix action statistics for firewall filters.</p> <p><b>terse</b>—Display firewall filter names only.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">show firewall on page 1039</a>                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Output Fields</b>            | <a href="#">Table 114 on page 1038</a> lists the output fields for the <b>show firewall</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                   |

**Table 114: show firewall Output Fields**

| Field Name    | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter</b> | <p>Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> 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 <b>-i</b> for an input filter or <b>-o</b> 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 <b>-in</b> for an input filter or <b>-out</b> 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Counters</b> | <p>Display filter counter information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of a filter counter that has been configured with the <b>counter</b> firewall filter action.</li> <li>• <b>Bytes</b>—Number of bytes that match the filter term under which the <b>counter</b> action is specified.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term under which the <b>counter</b> action is specified.</li> </ul>                                                                                                                                                 |
| <b>Policers</b> | <p>Display policer information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of policer.</li> <li>• <b>Bytes</b>—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.</li> <li>• <b>Packets</b>—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.</li> </ul> |

## 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

|                                 |                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system autorecovery state                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                     |
| <b>Description</b>              | Performs checks and shows status of all autorecovered items.                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">request system autorecovery state on page 273</a></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show system autorecovery state on page 1040</a>                                                                                                                                                                                         |
| <b>Output Fields</b>            | Table 34 on page 292 lists the output fields for the <b>show system autorecovery state</b> 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 1043](#)

**Output Fields** [Table 116 on page 1042](#) 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

|                                 |                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show system download &lt;download-id&gt;</code>                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                           |
| <b>Description</b>              | Display a brief summary of all the download instances along with their current state and extent of progress. If a <b>download-id</b> is provided, the command displays a detailed report of the particular download instance.             |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>download-id</b>—(Optional) The ID number of the download instance.</li> </ul>                                                                                                                   |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">request system download start on page 279</a></li> <li><i>Installation and Upgrade Guide for Security Devices</i></li> <li><i>Administration Guide for Security Devices</i></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show system download on page 1044</a><br><a href="#">show system download 1 on page 1045</a>                                                                                                                                  |
| <b>Output Fields</b>            | Table 36 on page 296 lists the output fields for the <b>show system download</b> 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)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system license<br><installed   keys   status   usage>                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | Display licenses and information about how licenses are used.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>none</b>—Display all license information.</p> <p><b>installed</b>—(Optional) Display installed licenses only.</p> <p><b>keys</b>—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.</p> <p><b>status</b>—(Optional) Display license status for a specified logical system or for all logical systems.</p> <p><b>usage</b>—(Optional) Display the state of licensed features.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                                                                               |
| <b>List of Sample Output</b>    | <p><a href="#">show system license on page 1047</a></p> <p><a href="#">show system license installed on page 1047</a></p> <p><a href="#">show system license keys on page 1048</a></p> <p><a href="#">show system license usage on page 1048</a></p> <p><a href="#">show system license status logical-system all on page 1048</a></p>                                                                                                                   |
| <b>Output Fields</b>            | Table 18 on page 121 lists the output fields for the <b>show system license</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                         |

**Table 118: show system license Output Fields**

| Field Name           | Field Description                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Feature name</b>  | Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.                                                                |
| <b>Licenses used</b> | 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"> <li>• <b>License identifier</b>—Identifier associated with a license key.</li> <li>• <b>License version</b>—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.</li> <li>• <b>Valid for device</b>—Device that can use a license key.</li> <li>• <b>Features</b>—Feature associated with a license.</li> </ul> |
| 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<br>01:00:00 IST | 1             | 1                  | 0               | 2012-03-30 |
| wf_key_surfcontrol_cpa<br>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<br>used | Licenses<br>installed | Licenses<br>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 login logout

|                                 |                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system login logout                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Release 11.2 of Junos OS.                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | Display the user names locked after unsuccessful login attempts.                                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | view and system                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Administration Guide for Security Devices</i></li> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                       |
| <b>List of Sample Output</b>    | <a href="#">show system login logout on page 1049</a>                                                                                                                                                                                                                                                            |
| <b>Output Fields</b>            | Table 38 on page 301 lists the output fields for the <b>show system login logout</b> 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 <b>detail</b> keyword is used. |

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

|                                 |                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show system services dhcp client</b><br><b>&lt; <i>interface-name</i> &gt;</b><br><b>&lt;statistics&gt;</b>                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 8.5.                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Display information about DHCP clients.                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• <b>none</b>—Display DHCP information for all interfaces.</li> <li>• <b><i>interface-name</i></b> —(Optional) Display DHCP information for the specified interface.</li> <li>• <b>statistics</b>—(Optional) Display DHCP client statistics.</li> </ul> |
| <b>Required Privilege Level</b> | view and system                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>dhcp (Interfaces)</i></li> <li>• <a href="#">request system services dhcp on page 987</a></li> <li>• <i>Administration Guide for Security Devices</i></li> </ul>                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show system services dhcp client on page 1051</a><br><a href="#">show system services dhcp client ge-0/0/1.0 on page 1052</a><br><a href="#">show system services dhcp client statistics on page 1052</a>                                                                          |
| <b>Output Fields</b>            | <a href="#">Table 19 on page 124</a> lists the output fields for the <b>show system services dhcp client</b> 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.          |

Table 120: show system services dhcp client Output Fields (*continued*)

| Field Name        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Options      | <ul style="list-style-type: none"> <li>• <b>Name:</b> server-identifier, <b>Value:</b> IP address of the name server.</li> <li>• <b>Name:</b> device, <b>Value:</b> IP address of the name device.</li> <li>• <b>Name:</b> domain-name, <b>Value:</b> Name of the domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Packets dropped   | Total packets dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Messages received | <p>Number of the following DHCP messages received:</p> <ul style="list-style-type: none"> <li>• <b>DHCPOFFER</b>—First packet received on a logical interface when DHCP is enabled.</li> <li>• <b>DHCPACK</b>—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.</li> <li>• <b>DHCPNAK</b>—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Messages sent     | <p>Number of the following DHCP messages sent:</p> <ul style="list-style-type: none"> <li>• <b>DHCPDECLINE</b>—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet.</li> <li>• <b>DHCPDISCOVER</b>—Packet sent on the interface for which the DHCP client is enabled.</li> <li>• <b>DHCPREQUEST</b>—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer.</li> <li>• <b>DHCPINFORM</b>—Packet sent to the DHCP server for local configuration parameters.</li> <li>• <b>DHCPRELEASE</b>—Packet sent to the DHCP server to relinquish network address and cancel remaining lease.</li> <li>• <b>DHCPRENEW</b>—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.</li> <li>• <b>DHCPREBIND</b>—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.</li> </ul> |

## 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

|                                 |                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show system services dhcp relay-statistics</b>                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Release 8.5 of Junos OS.                                                                                                                                                            |
| <b>Description</b>              | Display information about the DHCP relay.                                                                                                                                                                 |
| <b>Required Privilege Level</b> | view and system                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>dhcp</i></li> <li><i>Administration Guide for Security Devices</i></li> </ul>                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show system services dhcp relay-statistics on page 1053</a>                                                                                                                                   |
| <b>Output Fields</b>            | <a href="#">Table 121 on page 1053</a> lists the output fields for the <b>show system services dhcp relay-statistics</b> 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"> <li><b>Due to a missing interface in the relay database</b>—Number of packets discarded because they did not belong to a configured interface.</li> <li><b>Due to a missing matching routing instance</b>—Number of packets discarded because they did not belong to a configured routing instance.</li> <li><b>Due to an error during packet read</b>—Number of packets discarded because of a system read error.</li> <li><b>Due to an error during packet send</b>—Number of packets that the DHCP relay application could not send.</li> <li><b>Due to an invalid server address</b>—Number of packets discarded because an invalid server address was specified.</li> <li><b>Due to a missing valid local address</b>—Number of packets discarded because there was no valid local address.</li> <li><b>Due to a missing route to the server or client</b>—Number of packets discarded because there were no addresses available for assignment.</li> </ul> |

## 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

|                                 |                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system snapshot media <i>media-type</i>                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Command introduced in Release 10.2 of Junos OS.                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Display the snapshot information for both root partitions on SRX Series devices                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li>• internal— Show snapshot information from internal media.</li> <li>• usb— Show snapshot information from device connected to USB port.</li> <li>• external— Show snapshot information from the external compact flash. This option is available on the SRX650 Services Gateway.</li> </ul> |
| <b>Required Privilege Level</b> | View                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul>                                                                                                                                                                                                                     |

### 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 39 on page 303](#) 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                                       |
|-------------------|---------------------------------------------------------|
| <b>Avail</b>      | Amount of space available in the file system.           |
| <b>Capacity</b>   | Percentage of the file system space that is being used. |
| <b>Mounted on</b> | 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)

|                                 |                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show system storage partitions                                                                                 |
| <b>Release Information</b>      | Command introduced in Release 10.2 of Junos OS.                                                                |
| <b>Description</b>              | Displays the partitioning scheme details on SRX Series devices.                                                |
| <b>Required Privilege Level</b> | View                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Installation and Upgrade Guide for Security Devices</i></li> </ul> |

## 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
```

# Access Privilege Administration Guide

- [Overview on page 1059](#)
- [Configuration on page 1067](#)
- [Administration on page 1226](#)

## Overview

---

- [Introduction to Access Privileges on page 1059](#)

## Introduction to Access Privileges

- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Junos OS Login Classes Overview on page 1063](#)
- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

### 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 1059](#)
- [Allowing or Denying Individual Commands for Junos OS Login Classes on page 1062](#)

### *Junos OS Login Class Permission Flags*

The **permissions** statement specifies one or more of the permission flags listed in [Table 123 on page 1060](#). 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 123 on page 1060](#) 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 123: 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.                                                  |
| <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.                                                                                    |

Table 123: Login Class Permission Flags (*continued*)

| Permission Flag                       | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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.                                                                                                                                                                                                                                                                                          |
| <b>interface-control</b>              | <p>Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels:</p> <ul style="list-style-type: none"> <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 and becoming the superuser in the shell by using the <b>su root</b> command, and can halt and reboot the router 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.                                                                                                                                                                                                                                                                                     |

Table 123: Login Class Permission Flags (*continued*)

| Permission Flag           | Description                                                                                                                                                                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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.                                                                                                                                                                                                     |
| <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).                                                                                                                                                                                                                                                                     |

***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 1067](#)

#### Junos OS Login Classes Overview

All users who can log in to the router or switch must be in a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the router or switch
- 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 out

You can define any number of login classes and then apply one login class to an individual user account.

The Junos OS contains a few predefined login classes, which are listed in [Table 124 on page 1064](#). The predefined login classes cannot be modified.

**Table 124: Predefined System Login Classes**

| Login Class             | Permission Flag Set                    |
|-------------------------|----------------------------------------|
| operator                | clear, network, reset, trace, and view |
| read-only               | view                                   |
| superuser or super-user | 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

**Related Documentation**

- [Understanding Junos OS Access Privilege Levels on page 1059](#)

### 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 1059](#)
- [access on page 1079](#)
- [access-control on page 1080](#)
- [admin on page 1081](#)
- [admin-control on page 1082](#)
- [all-control on page 1082](#)
- [clear on page 1083](#)
- [configure on page 1116](#)
- [control on page 1116](#)
- [field on page 1117](#)
- [firewall on page 1117](#)
- [firewall-control on page 1118](#)
- [floppy on page 1119](#)
- [flow-tap on page 1119](#)
- [flow-tap-operation on page 1120](#)
- [idp-profiler-operation on page 1120](#)
- [interface on page 1120](#)
- [interface-control on page 1121](#)
- [maintenance on page 1122](#)
- [network on page 1128](#)
- [pgcp-session-mirroring on page 1130](#)
- [pgcp-session-mirroring-control on page 1130](#)
- [reset on page 1131](#)
- [rollback on page 1131](#)
- [routing on page 1132](#)
- [routing-control on page 1136](#)
- [secret on page 1140](#)

- [secret-control on page 1141](#)
- [security on page 1142](#)
- [security-control on page 1145](#)
- [shell on page 1149](#)
- [snmp on page 1149](#)
- [system on page 1149](#)
- [system-control on page 1151](#)
- [trace on page 1153](#)
- [trace-control on page 1158](#)
- [view on page 1163](#)
- [view-configuration on page 1225](#)

### 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 1067](#)
- [Example: Configuring Access Privilege Levels on page 1070](#)

- [Understanding Junos OS Access Privilege Levels on page 1059](#)

## Configuration

---

- [Configuring Access Privileges on page 1067](#)
- [Examples on page 1069](#)
- [User Permission Flags Reference on page 1078](#)

### Configuring Access Privileges

- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1069](#)

#### 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 1070](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Junos OS Login Classes Overview on page 1063](#)

#### 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 1074](#)

### 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 1067](#)
- [Example: Configuring Access Privilege Levels on page 1070](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)

### Examples

- [Example: Configuring Access Privilege Levels on page 1070](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 1070](#)

- [Example: Configuring Access Privileges for Operational Mode Commands on page 1074](#)
- [Example: Specifying Access Privileges Using allow/deny-configuration-regexps Statements on page 1075](#)

---

### 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 1067](#)

---

### 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 1070](#)
- [Overview on page 1070](#)
- [Configuration on page 1071](#)
- [Examples Using Allow or Deny Configurations with Regular Expressions on page 1071](#)

#### Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, 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 1067](#)
- [Example: Configuring Access Privilege Levels on page 1070](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)

### 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 1067](#)

### 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 1075](#)
- [Overview on page 1075](#)
- [Configuration on page 1075](#)
- [Examples Using Allow or Deny Configurations with Regular Expressions on page 1076](#)

#### Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, 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 1067](#)
  - [Example: Configuring Access Privilege Levels on page 1070](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)

## User Permission Flags Reference

- [access on page 1079](#)
- [access-control on page 1080](#)
- [admin on page 1081](#)
- [admin-control on page 1082](#)
- [all-control on page 1082](#)
- [clear on page 1083](#)
- [configure on page 1116](#)



- [control](#) on page 1116
- [field](#) on page 1117
- [firewall](#) on page 1117
- [firewall-control](#) on page 1118
- [floppy](#) on page 1119
- [flow-tap](#) on page 1119
- [flow-tap-control](#) on page 1119
- [flow-tap-operation](#) on page 1120
- [idp-profiler-operation](#) on page 1120
- [interface](#) on page 1120
- [interface-control](#) on page 1121
- [maintenance](#) on page 1122
- [network](#) on page 1128
- [pgcp-session-mirroring](#) on page 1130
- [pgcp-session-mirroring-control](#) on page 1130
- [reset](#) on page 1131
- [rollback](#) on page 1131
- [routing](#) on page 1132
- [routing-control](#) on page 1136
- [secret](#) on page 1140
- [secret-control](#) on page 1141
- [security](#) on page 1142
- [security-control](#) on page 1145
- [shell](#) on page 1149
- [snmp](#) on page 1149
- [system](#) on page 1149
- [system-control](#) on page 1151
- [trace](#) on page 1153
- [trace-control](#) on page 1158
- [view](#) on page 1163
- [view-configuration](#) on page 1225

## [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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [access-control on page 1080](#)

#### 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [access on page 1079](#)

## 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)

- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [admin-control on page 1082](#)

---

### admin-control

---

Can view user account information and configure it at the **[edit system]** hierarchy level.

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commands</b>                       | show system audit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Configuration Hierarchy Levels</b> | <ul style="list-style-type: none"><li>[edit protocols uplink-failure-detection]</li><li>[edit system]</li><li>[edit system accounting]</li><li>[edit system diag-port-authentication]</li><li>[edit system extensions]</li><li>[edit system login]</li><li>[edit system pic-console-authentication]</li><li>[edit system root-authentication]</li><li>[edit system services ssh ciphers]</li><li>[edit system services ssh hostkey-algorithm]</li><li>[edit system services ssh key-exchange]</li><li>[edit system services ssh macs]</li><li>[edit system services ssh protocol-version]</li><li>[edit system services ssh root-login]</li></ul> |
| <b>Related Documentation</b>          | <ul style="list-style-type: none"><li>• <a href="#">Access Privilege User Permission Flags Overview on page 1064</a></li><li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 1059</a></li><li>• <a href="#">Configuring Access Privilege Levels on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066</a></li><li>• <a href="#">admin on page 1081</a></li></ul>                                                                           |

---

### all-control

---

Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commands</b>                       | All CLI commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Configuration Hierarchy Levels</b> | All 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 1064</a></li><li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 1059</a></li><li>• <a href="#">Configuring Access Privilege Levels on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066</a></li></ul> |

## clear

Can clear (delete) information learned from the network that is stored in various network databases.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commands</b> | clear<br>clear amt<br>clear amt statistics<br><clear-amt-statistics><br>clear amt tunnel<br>clear-amt-tunnel<br>clear amt tunnel gateway-address<br><clear amt tunnel gateway-address><br>clear amt tunnel statistics<br><clear-amt-tunnel-statistics><br>clear amt tunnel statistics gateway-address<br><clear-amt-tunnel-gateway-address-statistics><br>clear amt tunnel statistics tunnel-interface<br><clear-amt-tunnel-interface-statistics><br>clear amt tunnel tunnel-interface<br><clear-amt-tunnel-interface<><br>clear ancp<br>clear ancp neighbor<br><clear-ancp-neighbor-connection><br>clear ancp subscriber<br><clear-ancp-subscriber-connection><br>clear arp<br><clear-arp-table><br>clear auto-configuration<br>clear auto-configuration interfaces<br><clear-auto-configuration-interfaces><br>clear bfd<br>clear bfd adaptation<br><clear-bfd-adaptation-information><br>clear bfd adaptation address<br><clear-bfd-adaptation-address><br>clear bfd adaptation discriminator<br><clear-bfd-adaptation-discriminator><br>clear bfd session<br><clear-bfd-session-information><br>clear bfd session address<br><clear-bfd-session-address><br>clear bfd session discriminator<br><clear-bfd-session-discriminator><br>clear bgp<br>clear bgp damping<br><clear-bgp-damping><br>clear bgp neighbor<br><clear-bgp-neighbor><br>clear bgp table<br><clear-bgp-table><br>clear bridge<br>clear bridge mac-table<br><clear-bridge-mac-table><br>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-lldp-aggregate-states
clear ddos-protection protocols lldp aggregate statistics
clear-ddos-lldp-aggregate-statistics
clear ddos-protection protocols lldp states
clear-ddos-lldp-states
clear ddos-protection protocols lldp statistics
clear-ddos-lldp-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 mplsdp
clear ddos-protection protocols ppp mplsdp states
clear-ddos-ppp-mplsdp-states
clear ddos-protection protocols ppp mplsdp statistics
clear-ddos-ppp-mplsdp-statistics
clear ddos-protection protocols ppp states
clear-ddos-ppp-states
clear ddos-protection protocols ppp statistics
clear-ddos-ppp-statistics
clear ddos-protection protocols ppp unclassified
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
<clear-ddos-ppp-unclass-statistics>
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
```

```
clear ddos-protection protocols pppoe aggregate states
clear-ddos-pppoe-aggregate-states
clear ddos-protection protocols pppoe aggregate statistics
clear-ddos-pppoe-aggregate-statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear-ddos-pppoe-padi-states
clear ddos-protection protocols pppoe padi statistics
clear-ddos-pppoe-padi-statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear-ddos-pppoe-padm-states
clear ddos-protection protocols pppoe padm statistics
clear-ddos-pppoe-padm-statistics
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
clear-ddos-pppoe-padn-states
clear ddos-protection protocols pppoe padn statistics
clear-ddos-pppoe-padn-statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear-ddos-pppoe-pado-states
clear ddos-protection protocols pppoe pado statistics
clear-ddos-pppoe-pado-statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear-ddos-pppoe-padr-states
clear ddos-protection protocols pppoe padr statistics
clear-ddos-pppoe-padr-statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear-ddos-pppoe-pads-states
clear ddos-protection protocols pppoe pads statistics
clear-ddos-pppoe-pads-statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear-ddos-pppoe-padt-states
clear ddos-protection protocols pppoe padt statistics
clear-ddos-pppoe-padt-statistics
clear ddos-protection protocols pppoe states
clear-ddos-pppoe-states
clear ddos-protection protocols pppoe statistics
clear-ddos-pppoe-statistics
clear ddos-protection protocols ptp
clear ddos-protection protocols ptp aggregate
clear ddos-protection protocols ptp aggregate states
clear-ddos-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 bpdu
clear error bpdu interface
<clear-bpdu-error>
clear error mac-rewrite
clear error mac-rewrite interface
<clear-mac-rewrite-error>
clear esis
clear esis adjacency
<clear-esis-adjacency>
clear esis statistics
<clear-esis-statistics>
clear fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
```

```
clear firewall all
<clear-all-firewall-conters>
clear firewall log
clear 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 software
```

```
clear services software statistics
<clear-services-software-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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

---

## 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

---

## 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

### 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

### firewall

---

Can view the firewall filter configuration in configuration mode.

**Commands**

```
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>
```

**Configuration  
Hierarchy Levels**      [\[edit dynamic-profiles firewall\]](#)  
                                 [\[edit firewall\]](#)  
                                 [\[edit logical-systems firewall\]](#)

- Related  
Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [firewall-control on page 1118](#)

### [firewall-control](#)

---

Can view and configure firewall filter information at the [\[edit dynamic-profiles firewall\]](#), [\[edit firewall\]](#), and [\[edit logical-systems firewall\]](#) hierarchy levels.

**Commands**

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

**Configuration  
Hierarchy Levels**      [\[edit dynamic-profiles firewall\]](#)  
                                 [\[edit firewall\]](#)  
                                 [\[edit logical-systems firewall\]](#)

- Related  
Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [firewall on page 1117](#)



### floppy

---

Can read from and write to the removable media.

**Commands** No associated CLI commands.

**Configuration Hierarchy Levels** No associated CLI configuration hierarchy levels and statements.

**Related Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

### flow-tap

---

Can view the flow-tap configuration in configuration mode.

**Commands** No associated CLI commands.

**Configuration Hierarchy Levels**

- [edit services flow-tap]
- [edit services radius-flow-tap]
- [edit system services flow-tap-dtcp]

**Related Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [flow-tap-control on page 1119](#)

### flow-tap-control

---

Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap], [edit services radius-flow-tap], and [edit system services flow-tap-dtcp] hierarchy levels.

**Commands** No associated CLI commands.

**Configuration Hierarchy Levels**

- [edit services flow-tap]
- [edit services radius-flow-tap]
- [edit system services flow-tap-dtcp]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [flow-tap on page 1119](#)

---

### flow-tap-operation

---

Can make flow-tap requests to the router.

**Commands** No associated CLI commands.

**Configuration Hierarchy Levels** No associated CLI configuration hierarchy levels and statements.

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

---

### 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [interface-control on page 1121](#)

### 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [interface on page 1120](#)

---

## **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 tfeb
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
```

	<pre>start shell start shell user test access test access profile   &lt;get-radius-profile-access-test-result&gt;  test access radius-server   &lt;get-radius-server-access-test-result&gt; get-test-services-l2tp-tunnel-result</pre>
<b>Configuration Hierarchy Levels</b>	<pre>[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]</pre>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Access Privilege User Permission Flags Overview on page 1064</a></li><li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 1059</a></li><li>• <a href="#">Configuring Access Privilege Levels on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067</a></li><li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066</a></li></ul>

---

## 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

---

### pgcp-session-mirroring

Can view session mirroring configuration by using the **pgcp** command.

**Commands** show services pgcp gates gate-way display session-mirroring

**Configuration Hierarchy Levels** [edit services pgcp gateway session-mirroring]  
[edit services pgcp session-mirroring]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [pgcp-session-mirroring-control on page 1130](#)

---

### 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
  - [pgcp-session-mirroring on page 1130](#)

## 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

## rollback

Can roll back to previous configurations.

**Commands** rollback

**Configuration Hierarchy Levels** [edit]

- Related Documentation**
- [Access Privilege User Permission Flags Overview on page 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)
  - [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
  - [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

## 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 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

- [routing-control on page 1136](#)

## 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.

<b>Configuration Hierarchy Levels</b>	[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-instances instance switch-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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [routing on page 1132](#)

## 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 1064](#)
  - [Understanding Junos OS Access Privilege Levels on page 1059](#)
  - [Configuring Access Privilege Levels on page 1067](#)

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [secret-control on page 1141](#)

### **secret-control**

Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.

**Commands** No associated CLI commands.

<b>Configuration Hierarchy Levels</b>	<p>[edit access profile client chap-secret]</p> <p>[edit access profile client firewall-user password]</p> <p>[edit access profile client l2tp shared-secret]</p> <p>[edit access profile client pap-password]</p> <p>[edit access profile radius-server secret]</p> <p>[edit access radius-disconnect secret]</p> <p>[edit dynamic-profiles interfaces interface ppp-options chap default-chap-secret]</p> <p>[edit dynamic-profiles interfaces interface ppp-options pap default-password]</p> <p>[edit dynamic-profiles interfaces interface ppp-options pap local-password]</p> <p>[edit dynamic-profiles interfaces interface unit ppp-options chap default-chap-secret]</p> <p>[edit dynamic-profiles interfaces interface unit ppp-options pap default-password]</p> <p>[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]</p> <p>[edit interfaces interface ppp-options chap default-chap-secret]</p> <p>[edit interfaces interface ppp-options pap default-password]</p> <p>[edit interfaces interface ppp-options pap local-password]</p> <p>[edit interfaces interface unit ppp-options chap default-chap-secret]</p> <p>[edit interfaces interface unit ppp-options pap default-password]</p> <p>[edit interfaces interface unit ppp-options pap local-password]</p> <p>[edit logical-systems interfaces interface unit ppp-options chap]</p> <p>[edit logical-systems interfaces interface unit ppp-options pap default-password]</p> <p>[edit logical-systems interfaces interface unit ppp-options pap local-password]</p> <p>[edit logical-systems routing-instances instance system services static-subscribers authentication password]</p> <p>[edit logical-systems routing-instances instance system services static-subscribers group authentication password]</p> <p>[edit logical-systems system services static-subscribers authentication password]</p> <p>[edit logical-systems system services static-subscribers group authentication password]</p> <p>[edit routing-instances instance system services static-subscribers authentication password]</p> <p>[edit routing-instances instance system services static-subscribers group authentication password]</p> <p>[edit services ggsn apn radius accounting server secret]</p> <p>[edit services ggsn apn radius authentication server secret]</p> <p>[edit services ggsn radius server secret]</p> <p>[edit system accounting destination radius server secret]</p> <p>[edit system accounting destination tacplus server secret]</p> <p>[edit system radius-server secret]</p> <p>[edit system services outbound-ssh client secret]</p> <p>[edit system services packet-triggered-subscribers partition-radius accounting-shared-secret]</p> <p>[edit system services static-subscribers authentication password]</p> <p>[edit system services static-subscribers group authentication password]</p>
---------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[edit system tacplus-server secret]

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [secret on page 1140](#)

---

## 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [security-control on page 1145](#)

## 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 crt
request security pki crt load
  <request security pki crt load>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
  <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
  <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
  <get-idp-application-system-cache>

show security idp application-statistics
  <get-idp-applications-information>

show security idp attack
show security idp attack description
  <get-idp-attack-description-information>
show security idp attack detail
  <get-idp-attack-detail-information>
show security idp attack table
  <get-idp-attack-table-information>

show security idp counters
  <get-idp-counter-information>

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
  <get-idp-memory-information>

show security idp policies
  <get-idp-subscriber-policy-list>

show security idp policy-templates-list
  <get-idp-policy-template-information>
```

```
<get-idp-predefined-attack-groups>
<get-idp-predefined-attack-group-filters>
<get-idp-predefined-attacks>
<get-idp-predefined-attack-filters>
<get-idp-recent-security-package-information>
show security idp policy-commit-status
  <get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp security-package-version
  <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
  <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>
```

**Configuration  
Hierarchy Levels**

```
[edit security]
[edit security alarms]
[edit security log]
```

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [security on page 1142](#)

---

## shell

Can start a local shell on the router.

<b>Commands</b>	start shell start shell user
<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 1064</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 1059</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 1067</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066</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 1064</a></li> <li>• <a href="#">Understanding Junos OS Access Privilege Levels on page 1059</a></li> <li>• <a href="#">Configuring Access Privilege Levels on page 1067</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067</a></li> <li>• <a href="#">Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066</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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [system-control on page 1151](#)

### system-control

Can view system-level configuration information and configure it at the **[edit system]** hierarchy level.

#### Configuration Hierarchy Levels

[\[edit applications\]](#)  
[\[edit chassis system-domains\]](#)  
[\[edit dynamic-profiles routing-instances instance forwarding-options helpers tftp\]](#)  
[\[edit dynamic-profiles routing-instances instance routing-options fate-sharing\]](#)  
[\[edit ethernet-switching-options\]](#)  
[\[edit forwarding-options helpers bootp\]](#)  
[\[edit forwarding-options helpers domain\]](#)  
[\[edit forwarding-options helpers port\]](#)  
[\[edit forwarding-options helpers tftp\]](#)  
[\[edit logical-systems\]](#)  
[\[edit logical-systems routing-instances instance forwarding-options helpers bootp\]](#)  
[\[edit logical-systems routing-instances instance forwarding-options helpers domain\]](#)  
[\[edit logical-systems routing-instances instance forwarding-options helpers port\]](#)  
[\[edit logical-systems routing-instances instance forwarding-options helpers tftp\]](#)  
[\[edit logical-systems routing-instances instance routing-options fate-sharing\]](#)  
[\[edit logical-systems routing-options fate-sharing\]](#)  
[\[edit logical-systems system\]](#)  
[\[edit poe\]](#)  
[\[edit routing-instances instance forwarding-options helpers bootp\]](#)  
[\[edit routing-instances instance forwarding-options helpers domain\]](#)  
[\[edit routing-instances instance forwarding-options helpers port\]](#)  
[\[edit routing-instances instance forwarding-options helpers tftp\]](#)  
[\[edit routing-instances instance routing-options fate-sharing\]](#)  
[\[edit routing-options fate-sharing\]](#)  
[\[edit services\]](#)  
[\[edit services ggsn charging charging-log traceoptions\]](#)

```
[edit system]
[edit system archival]
[edit system backup-router]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system processes]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
[edit vlans]
```

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [system on page 1149](#)

## 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]
[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 1064](#)

- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)
- [trace-control on page 1158](#)

## 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 isis 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 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

- [trace on page 1153](#)

## 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 ipv6
  get-ddos-ipv6-information
show ddos-protection protocols ipv6 aggregate
  get-ddos-ipv6-aggregate
show ddos-protection protocols ipv6 parameters
  get-ddos-ipv6-parameters
show ddos-protection protocols ipv6 statistics
  get-ddos-ipv6-statistics
show ddos-protection protocols ipv6 violations
  get-ddos-ipv6-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-sslv6-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-mspinf-info-connections>

show extension-provider system packages
  <get-mspinf-info-packages>

show extension-provider system processes
  <get-mspinf-info-processes>

show extension-provider system processes brief
  <get-mspinf-info-processes-brief>

show extension-provider system processes extensive
  <get-mspinf-info-processes-extensive>

show extension-provider system uptime
  <get-mspinf-info-uptime>

show extension-provider system virtual-memory
  <get-mspinf-info-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-ntp-slave>
show ntp statistics
  <get-ntp-statistics>
show r2cp
show r2cp interfaces
  <get-r2cp-interface-information>
show r2cp radio
  <get-r2cp-radio-information>
show r2cp sessions
  <get-r2cp-session-information>
show r2cp statistics
  <get-r2cp-statistics>
show redundant-power-system
show redundant-power-system led
show redundant-power-system multi-backup
<get-rps-scale-information>
show redundant-power-system network
<get-rps-network-information>
show redundant-power-system power-supply
show redundant-power-system status
show redundant-power-system upgrade
<get-rps-upgrade-information>
show redundant-power-system version
show rip
show rip general-statistics
  <get-rip-general-statistics-information>

show rip neighbor
  <get-rip-neighbor-information>

show rip statistics
  <get-rip-statistics-information>
show rip statistics peer
  <get-rip-peer-information>
show ripng
show ripng general-statistics
  <get-ripng-general-statistics-information>

show ripng neighbor
  <get-ripng-neighbor-information>
show ripng statistics
  <get-ripng-statistics-information>
show route
  <get-route-information>

show route export
  <get-rlexport-table-information>

show route export instance
  <get-rlexport-instance-information>

show route localization
  <get-fib-localization-information>
show route export vrf-target
  <get-rlexport-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

show 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
<

```

**Configuration  
Hierarchy Levels**

```

[edit dynamic-profiles routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems routing-instances instance services mobile-ip home-agent
enable-service]
[edit logical-systems services mobile-ip home-agent enable-service]
[edit routing-instances instance services mobile-ip home-agent enable-service]
[edit services mobile-ip home-agent enable-service]

```

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)
- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

### view-configuration

Can view all of the configuration (not including secrets).

**Commands**

No associated CLI commands.

**Configuration  
Hierarchy Levels**

No associated CLI configuration hierarchy levels and statements.

**Related  
Documentation**

- [Access Privilege User Permission Flags Overview on page 1064](#)
- [Understanding Junos OS Access Privilege Levels on page 1059](#)
- [Configuring Access Privilege Levels on page 1067](#)

- [Specifying Access Privileges for Junos OS Operational Mode Commands on page 1067](#)
- [Specifying Access Privileges for Junos OS Configuration Mode Hierarchies on page 1066](#)

## Administration

---

- [Operational Mode Commands on page 1226](#)

### Operational Mode Commands

- [show cli authorization](#)

## 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



## PART 6

# Monitoring and Troubleshooting Library for Security Devices

- [Network Monitoring and Troubleshooting Guide for Security Devices on page 1231](#)
- [System Log Monitoring and Troubleshooting Guide for Security Devices on page 1633](#)
- [SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices on page 1715](#)
- [IDP Monitoring and Troubleshooting Guide for Security Devices on page 1995](#)





## CHAPTER 18

# Network Monitoring and Troubleshooting Guide for Security Devices

- [Overview on page 1231](#)
- [Configuration on page 1253](#)
- [Administration on page 1354](#)
- [Troubleshooting on page 1611](#)

## Overview

---

- [Monitoring and Troubleshooting on page 1231](#)
- [Accounting, Source Class Usage, and Destination Class Usage Options on page 1235](#)
- [Alarms on page 1237](#)
- [Data Path Debugging and Trace Options on page 1242](#)
- [MPLS on page 1244](#)
- [Packet Capture on page 1246](#)
- [RPM on page 1248](#)

## Monitoring and Troubleshooting

- [Monitoring Overview on page 1231](#)
- [Diagnostic Tools Overview on page 1232](#)

### 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 1382](#)
- [Diagnostic Tools Overview on page 1232](#)

### 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 1233](#)
- [CLI Diagnostic Commands on page 1233](#)

### *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 125 on page 1233](#) describes the functions of the Troubleshoot options.

**Table 125: J-Web Interface Troubleshoot Options**

Option	Function
<b>Troubleshoot Options</b>	
<b>Ping Host</b>	Allows you to ping a remote host. You can configure advanced options for the ping operation.
<b>Ping MPLS</b>	Allows you to ping an MPLS endpoint using various options.
<b>Traceroute</b>	Allows you to trace a route between the device and a remote host. You can configure advanced options for the traceroute operation.
<b>Packet Capture</b>	Allows you to capture and analyze router control traffic.
<b>Maintain Options</b>	
<b>Files</b>	Allows you to manage log, temporary, and core files on the device.
<b>Upgrade</b>	Allows you to upgrade and manage Junos OS packages.
<b>Licenses</b>	Displays a summary of the licenses needed and used for each feature that requires a license. Allows you to add licenses.
<b>Reboot</b>	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 126 on page 1234](#).

**Table 126: CLI Diagnostic Command Summary**

Command	Function
<b>Controlling the CLI Environment</b>	
<b>set option</b>	Configures the CLI display.
<b>Diagnosis and Troubleshooting</b>	
<b>clear</b>	Clears statistics and protocol database information.
<b>mtrace</b>	Traces information about multicast paths from source to receiver.
<b>monitor</b>	Performs real-time debugging of various Junos OS components, including the routing protocols and interfaces.
<b>ping</b>	Determines the reachability of a remote network host.
<b>ping mpls</b>	Determines the reachability of an MPLS endpoint using various options.
<b>test</b>	Tests the configuration and application of policy filters and AS path regular expressions.
<b>traceroute</b>	Traces the route to a remote network host.
<b>Connecting to Other Network Systems</b>	
<b>ssh</b>	Opens secure shell connections.
<b>telnet</b>	Opens Telnet sessions to other hosts on the network.
<b>Management</b>	
<b>copy</b>	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.
<b>restart option</b>	Restarts the various system processes, including the routing protocol, interface, and SNMP processes.
<b>request</b>	Performs system-level operations, including stopping and rebooting the device and loading Junos OS images.
<b>start</b>	Exits the CLI and starts a UNIX shell.
<b>configuration</b>	Enters configuration mode.
<b>quit</b>	Exits the CLI and returns to the UNIX shell.

- Related Documentation**
- [MPLS Connection Checking Overview on page 1244](#)
  - [Configuring Ping MPLS on page 1281](#)
  - [Using the J-Web Ping Host Tool on page 1488](#)
  - [Using the ping Command on page 1486](#)

## Accounting, Source Class Usage, and Destination Class Usage Options

- [Accounting Options Overview on page 1235](#)
- [Understanding Source Class Usage and Destination Class Usage Options on page 1236](#)

### 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 127 on page 1235](#).

**Table 127: 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 1254](#)
  - [Configuring Accounting-Data Log Files on page 1257](#)
  - [Configuring the Interface Profile on page 1260](#)
  - [Configuring the Filter Profile on page 1263](#)
  - [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)

## 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).

Class-based filter match conditions are not supported on J Series Services Routers.

### Related Documentation

- [Configuring SCU or DCU on page 1267](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the MIB Profile on page 1272](#)
- [Configuring the Routing Engine Profile on page 1274](#)

## Alarms

- [Alarm Overview on page 1237](#)

### 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.



**NOTE:** The **ALARM** LED on J Series devices light yellow whether the alarm condition is major (red) or minor (yellow).

This section contains the following topics:

- [Alarm Types on page 1237](#)
- [Alarm Severity on page 1237](#)
- [Alarm Conditions on page 1238](#)

### 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 1238](#)
- [System Alarm Conditions on page 1241](#)

### Interface Alarm Conditions

[Table 128 on page 1238](#) 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 128: 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.	<b>ais</b>
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	<b>ylw</b>
Ethernet	Link is down	The physical link is unavailable.	<b>link-down</b>
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.	<b>failure</b>



Table 128: 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.	<b>cts-absent</b>
	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.	<b>dcd-absent</b>
	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.	<b>dsr-absent</b>
	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.	<b>loss-of-rx-clock</b>
	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.	<b>loss-of-tx-clock</b>
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.	<b>hw-down</b>
	Services link down	The link between the device and its services module is unavailable.	<b>linkdown</b>
	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.	<b>pic-hold-reset</b>
	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.	<b>pic-reset</b>
	Services module software down	A software problem has occurred on the device's services module.	<b>sw-down</b>

Table 128: 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.	<b>ais</b>
	Loss of signal (LOS)	No remote E3 signal is being received at the E3 interface.	<b>los</b>
	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.	<b>oof</b>
	Remote defect indication	An AIS, LOS, or OOF condition exists. This alarm applies only to E3 interfaces configured in frame mode.	<b>rdi</b>

Table 128: 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.	<b>ais</b>
	Excessive number of zeros	The bit stream received from the upstream host has more consecutive zeros than are allowed in a T3 frame.	<b>exz</b>
	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.	<b>ferf</b>
	Idle alarm	The Idle signal is being received from the remote endpoint.	<b>idle</b>
	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.	<b>lcv</b>
	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.	<b>lof</b>
	Loss of signal (LOS)	No remote T3 signal is being received at the T3 interface.	<b>los</b>
	Phase-locked loop out of lock	The clocking signals for the local and remote endpoints no longer operate in lock-step.	<b>pll</b>
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	<b>ylw</b>

**System Alarm Conditions**

[Table 129 on page 1241](#) lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 129: System Alarm Conditions and Corrective Actions

Alarm Type	Alarm Condition	Corrective Action
Configuration	The rescue configuration is not set.	Set the rescue configuration.

Table 129: 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><b>NOTE:</b> 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 1276](#)
  - [Monitoring Active Alarms on a Device on page 1477](#)
  - [Monitoring Alarms on page 1478](#)
  - [System Log Messages](#)

## Data Path Debugging and Trace Options

- [Understanding Data Path Debugging for SRX Series Devices on page 1242](#)
- [Understanding Security Debugging Using Trace Options on page 1243](#)
- [Understanding Flow Debugging Using Trace Options on page 1243](#)

### Understanding Data Path Debugging for SRX Series Devices

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 1243](#)
- [Understanding Flow Debugging Using Trace Options on page 1243](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1279](#)

### 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 1242](#)
- [Understanding Flow Debugging Using Trace Options on page 1243](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1279](#)
- [Debugging the Data Path \(CLI Procedure\) on page 1279](#)
- [Displaying Output for Security Trace Options on page 1481](#)

### 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 1242](#)
- [Understanding Security Debugging Using Trace Options on page 1243](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1281](#)

- [Debugging the Data Path \(CLI Procedure\) on page 1279](#)

## MPLS

- [MPLS Connection Checking Overview on page 1244](#)

### 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.

When you use the ping MPLS feature from a J Series device operating as the inbound (ingress) node at the entry point of an LSP or VPN, the router 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 J Series device receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

[Table 87 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 130: Options for Checking MPLS Connections**

J-Web Ping MPLS Tool	ping mpls Command	Purpose	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 J Series device pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the J Series device 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 J Series device pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the J Series device sends the ping requests through the first gateway.  Ping requests sent to LDP-signaled LSPs use only the master routing instance.

Table 130: 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 J Series 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 J Series 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 J Series 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 J series 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 J Series 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 J Series 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 J Series device pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address.	—

- Related Documentation**
- [Diagnostic Tools Overview on page 1232](#)
  - [Configuring Ping MPLS on page 1281](#)
  - [Using the J-Web Ping Host Tool on page 1488](#)
  - [Using the ping Command on page 1486](#)

## Packet Capture

- [Packet Capture Overview on page 1246](#)

### 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 1247](#)
- [Firewall Filters for Packet Capture on page 1247](#)



- [Packet Capture Files on page 1247](#)
- [Analysis of Packet Capture Files on page 1248](#)

### ***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 1282](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)

## **RPM**

- [RPM Overview on page 1248](#)
- [RPM Support for VPN Routing and Forwarding on page 1252](#)

#### **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 1249](#)
- [RPM Tests on page 1249](#)
- [Probe and Test Intervals on page 1250](#)
- [Jitter Measurement with Hardware Timestamping on page 1250](#)
- [RPM Statistics on page 1250](#)
- [RPM Thresholds and Traps on page 1252](#)
- [RPM for BGP Monitoring on page 1252](#)

### ***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.

### ***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 131 on page 1250](#).

**Table 131: RPM Statistics**

RPM Statistics	Description
Round-Trip Times	

Table 131: RPM Statistics (*continued*)

RPM Statistics	Description
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
<b>Inbound and Outbound Times (ICMP Timestamp Probes Only)</b>	
Minimum egress time	Shortest one-way time from the Juniper Networks device to the remote server, as measured over the course of the test
Maximum ingress time	Shortest one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Average egress time	Average one-way time from the Juniper Networks device to the remote server, as measured over the course of the test
Average ingress time	Average one-way time from the remote server to the Juniper Networks device, as measured over the course of the test
Standard deviation egress time	Standard deviation of the one-way times from the Juniper Networks device to the remote server, as measured over the course of the test
Standard deviation ingress time	Standard deviation of the one-way times from the remote server to the Juniper Networks device, as measured over the course of the test
Egress jitter	Difference between the maximum and minimum outbound times, as measured over the course of the test
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
<b>Probe Counts</b>	
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 1306](#)
- [RPM Support for VPN Routing and Forwarding on page 1252](#)
- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Monitoring RPM Probes on page 1507](#)
- [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1618](#)

---

### ***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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Monitoring RPM Probes on page 1507](#)

## Configuration

---

- [Accounting, Source Class Usage, and Destination Class Usage Options on page 1253](#)
- [Alarms on page 1276](#)
- [Data Path Debugging and Trace Options on page 1278](#)
- [MPLS on page 1281](#)
- [Packet Capture on page 1282](#)
- [RPM on page 1294](#)
- [Configuration Statements on page 1310](#)

### Accounting, Source Class Usage, and Destination Class Usage Options

- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)
- [Accounting Options Configuration on page 1254](#)
- [Configuring Accounting-Data Log Files on page 1257](#)
- [Configuring the Interface Profile on page 1260](#)
- [Configuring the Filter Profile on page 1263](#)
- [Example: Configuring a Filter Profile on page 1265](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1265](#)
- [Configuring SCU or DCU on page 1267](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the MIB Profile on page 1272](#)
- [Configuring the Routing Engine Profile on page 1274](#)

#### Configuration Statements at the [edit accounting-options] Hierarchy Level

---

This topic shows all possible configuration statements at the **[edit accounting-options]** hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

```
[edit]
accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    destination-classes {
      destination-class-name;
    }
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
```

```
    }
    files number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
}
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
mib-profile profile-name {
  file filename;
  interval seconds;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

**Related  
Documentation**

- [Accounting Options Overview on page 1235](#)
- [Accounting Options Configuration on page 1254](#)

---

## Accounting Options Configuration

This topic contains the following sections:

- [Accounting Options—Full Configuration on page 1254](#)
- [Minimum Accounting Options Configuration on page 1256](#)

### **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 1235](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Configuring Accounting-Data Log Files on page 1257](#)
- [Configuring the Interface Profile on page 1260](#)
- [Configuring the Filter Profile on page 1263](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)

### 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 1258](#)
- [Configuring the Maximum Size of the File on page 1259](#)
- [Configuring the Maximum Number of Files on page 1259](#)
- [Configuring the Start Time for File Transfer on page 1259](#)
- [Configuring the Transfer Interval of the File on page 1259](#)
- [Configuring Archive Sites on page 1260](#)

### **Configuring the Storage Location of the File**

On J Series Services Routers, the files are stored by default on the compact flash drive. To configure the storage location of the files in the **mfs/var/log** directory (on DRAM) instead of the **cf/var/log** directory (on the compact flash drive), include the **nonpersistent** statement at the **[edit accounting-options file filename]** hierarchy level:

```

[edit accounting-options file filename]
nonpersistent;

```

This feature is useful for minimizing read/write traffic on the router's compact flash drive.



**NOTE:** If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. Therefore, you should back up these files periodically.

### Configuring the Maximum Size of the File

To configure the maximum size of the files, include the **size** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
size bytes;
```

The **size** statement is the maximum size of the log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). The minimum value for **bytes** is 256 KB. You must configure **bytes**; the remaining attributes are optional.

### Configuring the Maximum Number of Files

To configure the maximum number of files, include the **files** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
files number;
```

When a log file (for example, **profilelog**) reaches its maximum size, it is renamed **profilelog.0**, then **profilelog.1**, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for **number** is 3 and the default value is 10.

### Configuring the Start Time for File Transfer

To configure the start time for transferring files, include the **start-time** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
start-time time;
```

The start-time statement specifies a start time for file transfer (YYYY-MM-DD.hh:mm). For example, 10:00 a.m. on January 30, 2007 is represented as 2007-01-30.10:00.

### Configuring the Transfer Interval of the File

To configure the transfer interval of the files, include the **transfer-interval** statement at the **[edit accounting-options file filename]** hierarchy level:

```
[edit accounting-options file filename]
transfer-interval minutes;
```

The range for **transfer-interval** is 5 through 2880 minutes. The default is 30 minutes.



#### TIP:

Junos OS saves the existing log file and creates a new file at the configured transfer-intervals irrespective of:

- Whether the file has reached the maximum size or not
- Whether an archive site is configured or not

When you have a relatively smaller transfer-interval configured and if no archive site is configured, 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 1235](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Accounting Options Configuration on page 1254](#)
- [Configuring the Interface Profile on page 1260](#)
- [Configuring the Filter Profile on page 1263](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)

---

### 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 1261](#)
- [Configuring the File Information on page 1261](#)
- [Configuring the Interval on page 1261](#)
- [Example: Configuring the Interface Profile on page 1262](#)

### 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 1235](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Accounting Options Configuration on page 1254](#)
- [Configuring Accounting-Data Log Files on page 1257](#)
- [Configuring the Filter Profile on page 1263](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)

### 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 1263](#)
- [Configuring the File Information on page 1264](#)
- [Configuring the Interval on page 1264](#)

#### 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 1235](#)
- [Understanding Device Management Functions in Junos OS](#)
- [Accounting Options Configuration on page 1254](#)
- [Configuring Accounting-Data Log Files on page 1257](#)
- [Configuring the Interface Profile on page 1260](#)
- [Configuration Statements at the \[edit accounting-options\] Hierarchy Level on page 1253](#)
- [Example: Configuring a Filter Profile on page 1265](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1265](#)

### 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 1263](#)
- [Example: Configuring Interface-Specific Firewall Counters and Filter Profiles on page 1265](#)

### 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 1263](#)
- [Configuring the Interface Profile on page 1260](#)

## 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 1267](#)
- [Applying the Policy to the Forwarding Table on page 1267](#)
- [Enabling Accounting on Inbound and Outbound Interfaces on page 1267](#)

### *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 1236](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the MIB Profile on page 1272](#)
- [Configuring the Routing Engine Profile on page 1274](#)

### 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 1269](#)
- [Example: Mapping the VRF Instance Type to the Virtual Loopback Tunnel Interface on page 1269](#)
- [Example: Sending Traffic Received from the Virtual Loopback Interface Out the Source Class Output Interface on page 1270](#)

#### **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 1236](#)
- [Configuring SCU or DCU on page 1267](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the MIB Profile on page 1272](#)
- [Configuring the Routing Engine Profile on page 1274](#)

## Configuring Class Usage Profiles

To collect class usage statistics, perform the tasks described in these sections:

- [Configuring a Class Usage Profile on page 1270](#)
- [Configuring the File Information on page 1271](#)
- [Configuring the Interval on page 1271](#)
- [Creating a Class Usage Profile to Collect Source Class Usage Statistics on page 1271](#)
- [Creating a Class Usage Profile to Collect Destination Class Usage Statistics on page 1272](#)

### Configuring a Class Usage Profile

You can configure the class usage profile to collect statistics for particular source and destination classes.

To configure the class usage profile to filter by source classes, include the `source-classes` statement at the `[edit accounting-options class-usage-profile profile-name]` hierarchy level:

```
[edit accounting-options class-usage-profile profile-name]
source-classes {
```



```

    source-class-name;
}

```

To configure the class usage profile to filter by destination classes, include the **destination-classes** statement at the **[edit accounting-options class-usage-profile profile-name]** hierarchy level:

```

[edit accounting-options class-usage-profile profile-name]
destination-classes {
    destination-class-name;
}

```

### Configuring the File Information

Each accounting profile logs its statistics to a file in the **/var/log** directory.

To specify which file to use, include the **file** statement at the **[edit accounting-options class-usage-profile profile-name]** hierarchy level:

```

[edit accounting-options class-usage-profile profile-name]
file filename;

```

You must specify a filename for the source class usage profile that has already been configured at the **[edit accounting-options]** hierarchy level. You can also specify a filename for the destination class usage profile configured at the **[edit accounting-options]** hierarchy level.

### Configuring the Interval

Each interface with a class usage profile enabled has statistics collected once per interval specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the **interval** statement at the **[edit accounting-options class-usage-profile profile-name]** hierarchy level:

```

[edit accounting-options class-usage-profile profile-name]
interval;

```

### Creating a Class Usage Profile to Collect Source Class Usage Statistics

To create a class usage profile to collect source class usage statistics:

```

[edit]
accounting-options {
    class-usage-profile scu-profile1;
    file usage-stats;
    interval 15;
    source-classes {
        gold;
        silver;
        bronze;
    }
}

```

The class usage profile, **scu-profile1**, writes data to the file **usage\_stats**. The file might look like the following:

```

#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, scu_profile,epoch-timestamp,interface-name,source-class,
packet-count,byte-count
scu_profile,980313078,xe-1/0/0.0,gold,82,6888

```

```

scu_profile,980313078,xe-1/0/0.0,silver,164,13776
scu_profile,980313078,xe-1/0/0.0,bronze,0,0
scu_profile,980313678,xe-1/0/0.0,gold,82,6888
scu_profile,980313678,xe-1/0/0.0,silver,246,20664
scu_profile,980313678,xe-1/0/0.0,bronze,0,0

```

### ***Creating a Class Usage Profile to Collect Destination Class Usage Statistics***

To create a class usage profile to collect destination class usage statistics:

```

[edit]
accounting-options {
  class-usage-profile dcu-profile1;
  file usage-stats
  interval 15;
  destination-classes {
    gold;
    silver;
    bronze;
  }
}

```

The class usage profile, **dcu-profile1**, writes data to the file **usage-stats**. The file might look like the following:

```

#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, dcu_profile,epoch-timestamp,interface-name,destination-class,
packet-count,byte-count
dcu_profile,980313078,xe-1/0/0.0,gold,82,6888
dcu_profile,980313078,xe-1/0/0.0,silver,164,13776
dcu_profile,980313078,xe-1/0/0.0,bronze,0,0
dcu_profile,980313678,xe-1/0/0.0,gold,82,6888
dcu_profile,980313678,xe-1/0/0.0,silver,246,20664
dcu_profile,980313678,xe-1/0/0.0,bronze,0,0
...
#FILE CLOSED 976826178 2000-12-14-20:36:18

```

#### **Related Documentation**

- [Understanding Source Class Usage and Destination Class Usage Options on page 1236](#)
- [Configuring SCU or DCU on page 1267](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring the Routing Engine Profile on page 1274](#)

### **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 1273](#)
- [Configuring the Interval on page 1273](#)
- [Configuring the MIB Operation on page 1273](#)
- [Configuring MIB Object Names on page 1273](#)
- [Example: Configuring a MIB Profile on page 1274](#)

### 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 1236](#)
- [Configuring SCU or DCU on page 1267](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the Routing Engine Profile on page 1274](#)

---

### **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 1275](#)
- [Configuring the File Information on page 1275](#)
- [Configuring the Interval on page 1275](#)
- [Example: Configuring a Routing Engine Profile on page 1275](#)

### 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 1236](#)
- [Configuring SCU or DCU on page 1267](#)
- [Configuring SCU on a Virtual Loopback Tunnel Interface on page 1269](#)
- [Configuring Class Usage Profiles on page 1270](#)
- [Configuring the MIB Profile on page 1272](#)

## Alarms

- [Example: Configuring Interface Alarms on page 1276](#)

### Example: Configuring Interface Alarms

This example shows how to configure interface alarms.

- [Requirements on page 1276](#)
- [Overview on page 1276](#)
- [Configuration on page 1277](#)
- [Verification on page 1278](#)

#### **Requirements**

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1237](#).

#### **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 1237](#)
- [Monitoring Active Alarms on a Device on page 1477](#)
- [Monitoring Alarms on page 1478](#)

## Data Path Debugging and Trace Options

- [Debugging the Data Path \(CLI Procedure\) on page 1279](#)
- [Setting Security Trace Options \(CLI Procedure\) on page 1279](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1281](#)



### 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 1242](#)
- [Understanding Security Debugging Using Trace Options on page 1243](#)
- [Understanding Flow Debugging Using Trace Options on page 1243](#)
- [Setting Flow Debugging Trace Options \(CLI Procedure\) on page 1281](#)

### 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 1243](#)
- [Displaying Output for Security Trace Options on page 1481](#)

### 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 1243](#)

### MPLS

- [Configuring Ping MPLS on page 1281](#)

### 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 J Series 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 J Series 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 J Series 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 J Series device interfaces. If it is not a valid J Series device address, the ping request fails with the error message "Can't assign requested address."

**Related Documentation**

- [Diagnostic Tools Overview on page 1232](#)
- [MPLS Connection Checking Overview on page 1244](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- [Using the ping Command on page 1486](#)

## Packet Capture

- [Example: Enabling Packet Capture on a Device on page 1282](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
- [Example: Configuring Packet Capture for Datapath Debugging on page 1289](#)
- [Disabling Packet Capture on page 1292](#)
- [Deleting Packet Capture Files on page 1292](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1293](#)

### 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 1282](#)
- [Overview on page 1283](#)
- [Configuration on page 1283](#)
- [Verification on page 1284](#)

#### **Requirements**

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1284](#)
- [Verifying Captured Packets on page 1284](#)

### **Verifying the Packet Capture Configuration**

**Purpose** Verify that the packet capture is configured on the device.

**Action** From configuration mode, enter the **show forwarding-options** command. Verify that the output shows the intended file configuration for capturing packets.

### **Verifying Captured Packets**

**Purpose** Verify that the packet capture file is stored under the **/var/tmp** directory and the packets can be analyzed offline.

**Action** 1. Disable packet capture.

Using FTP, transfer a packet capture file (for example, **126b.fe-0.0.1**), to a server where you have installed packet analyzer tools (for example, **tools-server**).

a. From configuration mode, connect to **tools-server** using FTP.

```
[edit]
user@host# run ftp tools-server
Connected to tools-server.mydomain.net
220 tools-server.mydomain.net FTP server (Version 6.00LS) ready
Name (tools-server:user):remoteuser
331 Password required for remoteuser.
Password:
230 User remoteuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

b. Navigate to the directory where packet capture files are stored on the device.

```
ftp> lcd /var/tmp
Local directory now /cf/var/tmp
```

c. Copy the packet capture file that you want to analyze to the server, for example **126b.fe-0.0.1**.

```
ftp> put 126b.fe-0.0.1
```

```

local: 126b.fe-0.0.1 remote: 126b.fe-0.0.1
200 PORT command successful.
150 Opening BINARY mode data connection for '126b.fe-0.0.1'.
100% 1476 00:00 ETA
226 Transfer complete.
1476 bytes sent in 0.01 seconds (142.42 KB/s)

```

- d. Return to configuration mode.

```

ftp> bye
221 Goodbye.
[edit]
user@host#

```

2. Open the packet capture file on the server with tcpdump or any packet analyzer that supports libpcap format and review the output.

```

root@server% tcpdump -r 126b.fe-0.0.1 -xvvvv
01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl 64, id 33133, offset 0, flags [none], proto: ICMP (1),
length: 84) 14.1.1.1 > 15.1.1.1: ICMP echo request seq 0, length 64
    0005 85c8 f6d1 0005 85c4 e3d1 0800 4500
    0054 816d 0000 4001 da38 0e01 0101 0f01
    0101 0800 3c5a 981e 0000 8b5d 4543 51e6
    0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
    aaaa aaaa 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000
    0000
01:12:36.279793 Out 0:5:85:c8:f6:d1 > 0:5:85:c4:e3:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl 63, id 41227, offset 0, flags [none], proto: ICMP (1),
length: 84) 15.1.1.1 > 14.1.1.1: ICMP echo reply seq 0, length 64
    0005 85c4 e3d1 0005 85c8 f6d1 0800 4500
    0054 a10b 0000 3f01 bb9a 0f01 0101 0e01
    0101 0000 445a 981e 0000 8b5d 4543 51e6
    0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
    aaaa aaaa 0000 0000 0000 0000 0000 0000
    0000 0000 0000 0000 0000 0000 0000 0000
    0000
root@server%

```

#### Related Documentation

- [Packet Capture Overview on page 1246](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
- [Disabling Packet Capture on page 1292](#)
- [Deleting Packet Capture Files on page 1292](#)
- [Disabling Packet Capture on page 1292](#)

## Example: Configuring Packet Capture on an Interface

This example shows how to configure packet capture on an interface to analyze traffic.

- [Requirements on page 1286](#)
- [Overview on page 1286](#)
- [Configuration on page 1286](#)
- [Verification on page 1287](#)

### Requirements

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1246](#)
  - [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1293](#)
  - [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
  - [Example: Enabling Packet Capture on a Device on page 1282](#)
  - [Deleting Packet Capture Files on page 1292](#)
  - [Disabling Packet Capture on page 1292](#)

---

### **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 1287](#)
- [Overview on page 1287](#)
- [Configuration on page 1288](#)
- [Verification on page 1289](#)

#### **Requirements**

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1246](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Enabling Packet Capture on a Device on page 1282](#)
- [Deleting Packet Capture Files on page 1292](#)
- [Disabling Packet Capture on page 1292](#)

---

### **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 1289](#)
- [Overview on page 1289](#)
- [Configuration on page 1289](#)
- [Verification on page 1291](#)

### **Requirements**

Before you begin, see “[Debugging the Data Path \(CLI Procedure\)](#)” on page 1279.

### **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.

```
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*.

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 1291](#)
- [Verifying data path debugging capture on page 1291](#)
- [Verifying data path debugging counter on page 1292](#)

### **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
```

#### *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 1246](#)
  - [Understanding Data Path Debugging for SRX Series Devices on page 1242](#)
  - [Debugging the Data Path \(CLI Procedure\) on page 1279](#)

---

### 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 1246](#)
  - [Example: Configuring Packet Capture on an Interface on page 1286](#)
  - [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
  - [Example: Enabling Packet Capture on a Device on page 1282](#)
  - [Deleting Packet Capture Files on page 1292](#)

---

### 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 1292](#)).
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 1282](#)).
4. If you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [Packet Capture Overview on page 1246](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
- [Example: Enabling Packet Capture on a Device on page 1282](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1293](#)
- [Disabling Packet Capture on page 1292](#)

### 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 1292](#)).
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 1282](#)).
7. If you are done configuring the device, enter **commit** from configuration mode.

#### Related Documentation

- [Packet Capture Overview on page 1246](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)
- [Example: Configuring a Firewall Filter for Packet Capture on page 1287](#)
- [Example: Enabling Packet Capture on a Device on page 1282](#)

## RPM

- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1298](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1301](#)
- [Directing RPM Probes to Select BGP Devices on page 1303](#)
- [Configuring RPM Timestamping on page 1304](#)
- [Tuning RPM Probes on page 1305](#)
- [RPM Configuration Options on page 1306](#)

### Example: Configuring Basic RPM Probes

This example shows how to configure basic RPM probes to measure performance between two network endpoints.

- [Requirements on page 1295](#)
- [Overview on page 1295](#)
- [Configuration on page 1295](#)
- [Verification on page 1297](#)



### Requirements

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1297](#)
- [Verifying RPM Statistics on page 1297](#)

### 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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Tuning RPM Probes on page 1305](#)

---

**Example: Configuring RPM Using TCP and UDP Probes**

---

This example shows how to configure RPM using TCP and UDP probes.

- [Requirements on page 1298](#)
- [Overview on page 1298](#)
- [Configuration on page 1299](#)
- [Verification on page 1300](#)

**Requirements**

Before you begin:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See *Junos OS Interfaces Library 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 1294](#).

**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.



**NOTE:** On J Series devices, the destination interface must be an lt services 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.

```
{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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1301](#)
- [Tuning RPM Probes on page 1305](#)

---

### Example: Configuring RPM Probes for BGP Monitoring

This example shows how to configure RPM probes to monitor BGP neighbors.

- [Requirements on page 1301](#)
- [Overview on page 1301](#)
- [Configuration on page 1302](#)
- [Verification on page 1303](#)

#### **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 1294](#).
- 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 1298](#).

#### **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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Directing RPM Probes to Select BGP Devices on page 1303](#)
- [Tuning RPM Probes on page 1305](#)

### **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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1301](#)
- [Tuning RPM Probes on page 1305](#)

---

### 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 1248](#)
- [RPM Configuration Options on page 1306](#)
- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1298](#)
- [Tuning RPM Probes on page 1305](#)

### 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 1294.

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 1248](#)
  - [RPM Configuration Options on page 1306](#)
  - [Example: Configuring RPM Probes for BGP Monitoring on page 1301](#)
  - [Configuring RPM Timestamping on page 1304](#)

### RPM Configuration Options

You can configure real-time performance monitoring (RPM) parameters. See [Table 132 on page 1306](#) for a summary of the configuration options.

**Table 132: 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> |

Table 132: RPM Configuration Summary (*continued*)

| Field                           | Function   | Your Action  |
|---------------------------------|--|--|
| Interval                        | Sets the wait time (in seconds) between each probe transmission  | Type a number between 1 and 255 (seconds).   |
| Test Interval (required)        | Sets the wait time (in seconds) between tests.   | Type a number between 0 and 86400 (seconds).   |
| Probe Count                     | Sets the total number of probes to be sent for each test.  | Type a number between 1 and 15.  |
| Destination Port                | Specifies the TCP or UDP port to which probes are sent.<br><br>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).   |

Table 132: RPM Configuration Summary (*continued*)

| Field                              | Function   | Your Action   |
|------------------------------------|--|---|
| Jitter                             | Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.   | Type a number between 0 and 60,000,000 (microseconds).  |
| Standard Deviation                 | Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.                   | Type a number between 0 and 60,000,000 (microseconds).  |
| 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> |

Table 132: RPM Configuration Summary (*continued*)

| Field                               | Function   | Your Action   |
|-------------------------------------|--|---|
| Ingress Standard Deviation Exceeded | Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded. | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| Ingress Time Exceeded               | Generates traps when the threshold for maximum inbound time is exceeded.                     | <ul style="list-style-type: none"> <li>To enable SNMP traps for this condition, select the check box.</li> <li>To disable SNMP traps, clear the check box.</li> </ul> |
| 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 1248](#)
- [Example: Configuring Basic RPM Probes on page 1294](#)
- [Example: Configuring RPM Using TCP and UDP Probes on page 1298](#)
- [Example: Configuring RPM Probes for BGP Monitoring on page 1301](#)

## Configuration Statements

- Configuration Statements at the [edit accounting-options] Hierarchy Level on page 1311
- [edit security alarms] Hierarchy Level on page 1312
- [edit security datapath-debug] Hierarchy Level on page 1313
- [edit security traceoptions] Hierarchy Level on page 1314
- accounting-options on page 1315
- action-profile on page 1316
- archive-sites on page 1317
- capture-file (Security) on page 1318
- class-usage-profile on page 1319
- counters on page 1320
- datapath-debug on page 1321
- decryption-failures on page 1322
- destination-classes on page 1323
- destination-interface on page 1324
- destination-port on page 1325
- fields (for Interface Profiles) on page 1326
- fields (for Routing Engine Profiles) on page 1327
- file (Associating with a Profile) on page 1328
- file (Configuring a Log File) on page 1329
- files on page 1330
- filter-profile on page 1330
- flow (Security Flow) on page 1331
- hardware-timestamp on page 1333
- idp (Security Alarms) on page 1333
- interface-profile on page 1334
- interval on page 1335
- maximum-capture-size (Datapath Debug) on page 1336
- mib-profile on page 1336
- mpls (Security Forwarding Options) on page 1337
- next-hop on page 1337
- nonpersistent on page 1338
- object-names on page 1338
- operation on page 1339
- packet-capture on page 1340
- packet-filter on page 1341



- [probe](#) on page 1342
- [probe-interval](#) on page 1343
- [probe-limit](#) on page 1343
- [probe-server](#) on page 1344
- [probe-type](#) on page 1345
- [routing-engine-profile](#) on page 1346
- [rpm \(Services\)](#) on page 1347
- [size](#) on page 1349
- [source-classes](#) on page 1349
- [start-time](#) on page 1350
- [target](#) on page 1350
- [thresholds](#) on page 1351
- [traceoptions \(Security Datapath Debug\)](#) on page 1352
- [transfer-interval](#) on page 1353
- [traps](#) on page 1354

### Configuration Statements at the `[edit accounting-options]` Hierarchy Level

This topic shows all possible configuration statements at the `[edit accounting-options]` hierarchy level and their level in the configuration hierarchy. When you are configuring Junos OS, your current hierarchy level is shown in the banner on the line preceding the `user@host#` prompt.

```
[edit]
accounting-options {
  class-usage-profile profile-name {
    file filename;
    interval minutes;
    destination-classes {
      destination-class-name;
    }
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
    }
    files number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
  }
}
```

```
    file filename;
    interval minutes;
  }
}
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
mib-profile profile-name {
  file filename;
  interval seconds;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
routing-engine-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

**Related  
Documentation**

- [Accounting Options Overview on page 1235](#)
- [Accounting Options Configuration on page 1254](#)

---

**[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 58](#)
  - *IPsec VPN Feature Guide for Security Devices*
  - *IDP Policies Feature Guide for Security Devices*

#### [\[edit security datapath-debug\] 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 58](#)
- *Master Administrator for Logical Systems Feature Guide for Security Devices*

#### [\[edit security traceoptions\] 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 58](#)

---

## accounting-options

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | accounting-options {...}<br>}  |
| <b>Hierarchy Level</b>          | [edit]   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.  |
| <b>Description</b>              | Configure options for accounting statistics collection.  |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuration Statements at the [edit accounting-options] Hierarchy Level on page 1253</a></li><li>• <a href="#">Accounting Options Configuration on page 1254</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.

|                                 |  |
|---------------------------------|--|
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Network Monitoring and Troubleshooting Guide for Security Devices</i></li><li>• <a href="#">Example: Configuring Packet Capture for Datapath Debugging on page 1289</a></li></ul> |

---

## archive-sites

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>archive-sites {<br/>    <i>site-name</i>;<br/>}</pre>  |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format <i>router-name_log-filename_timestamp</i> . |
| <b>Options</b>                  | <i>site-name</i> —Any valid FTP URL to a destination.   |
| <b>Required Privilege Level</b> | snmp—To view this statement in the configuration.<br>snmp-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Archive Sites on page 1260</a></li></ul>  |

## capture-file (Security)

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>capture-file {<br/>    filename;<br/>    files number;<br/>    format <i>pcap-format</i>;<br/>    size <i>maximum-file-size</i>;<br/>    (world-readable   no-world-readable);<br/>}</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.<br/><br/>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.<br/><br/>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.<br/><br/>If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and a filename.<br/><br/>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 world-readable option enables any user to read the file. To explicitly set the default behavior, use the no-world-readable option.</li></ul> |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Junos OS Intrusion Detection and Prevention (IDP) Library for Security Devices</i></li><li>• <a href="#">System Log Messages</a></li></ul>   |



## class-usage-profile

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>class-usage-profile <i>profile-name</i> {   file <i>filename</i>;   interval <i>minutes</i>;   source-classes {     <i>source-class-name</i>;   }   destination-classes {     <i>destination-class-name</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 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. |
| <b>Options</b>                  | <p><b><i>profile-name</i></b>—Name of the destination class 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 Class Usage Profiles on page 1270</a></li> </ul>  |

## counters

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>counters {<br/>    counter-name;<br/>}</pre>   |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">filter-profile</a> <i>profile-name</i> ]   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the <code>/var/log</code> directory. |
| <b>Options</b>                  | <i>counter-name</i> —Name of the counter.   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Counters on page 1263</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.   |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li></ul> |

---

## decryption-failures

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>decryption-failures {<br/>    threshold <i>value</i>;<br/>}</pre>  |
| <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>                  | <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.<br><b>Range:</b> 0 through 1 through 1,000,000,000.<br><b>Default:</b> 1000                    |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Dynamic VPN Feature Guide for SRX Series Gateway Devices</i></li><li>• <i>Group VPN Feature Guide for Security Devices</i></li><li>• <i>IPsec VPN Feature Guide for Security Devices</i></li></ul> |

## destination-classes

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <code>destination-classes {<br/>    <i>destination-class-name</i>;<br/>}</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.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Specify the destination classes for which statistics are collected.   |
| <b>Options</b>                  | <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.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a Class Usage Profile on page 1270</a></li></ul>          |

## destination-interface

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <code>destination-interface <i>interface-name</i>;</code>   |
| <b>Hierarchy Level</b>          | [edit services ( rpm probe owner test <i>test-name</i> ),<br>[edit services rpm probe-server (tcp   udp)]]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.   |
| <b>Description</b>              | <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> |
| <b>Options</b>                  | <i>interface-name</i> —Name of the adaptive services interface.   |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">hardware-timestamp on page 1333</a></li> </ul>   |

## destination-port

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <code>destination-port <i>port</i>;</code>   |
| <b>Hierarchy Level</b>          | [edit services rpm bgp],<br>[edit services rpm probe <i>owner</i> test <i>test-name</i> ]  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>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 to 65,535.  |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |

## fields (for Interface Profiles)

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>fields {<br/>    <i>field-name</i>;<br/>}</pre>  |
| <b>Hierarchy Level</b>          | [edit accounting-options <b>interface-profile</b> <i>profile-name</i> ]   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Statistics to collect in an accounting-data log file for an interface.  |
| <b>Options</b>                  | <p><i>field-name</i>—Name of the field:</p> <ul style="list-style-type: none"><li>• <b>input-bytes</b>—Input bytes</li><li>• <b>input-errors</b>—Generic input error packets</li><li>• <b>input-multicast</b>—Input packets arriving by multicast</li><li>• <b>input-packets</b>—Input packets</li><li>• <b>input-unicast</b>—Input unicast packets</li><li>• <b>output-bytes</b>—Output bytes</li><li>• <b>output-errors</b>—Generic output error packets</li><li>• <b>output-multicast</b>—Output packets sent by multicast</li><li>• <b>output-packets</b>—Output packets</li><li>• <b>output-unicast</b>—Output unicast packets</li></ul> |
| <b>Required Privilege Level</b> | <b>interface</b> —To view this statement in the configuration.<br><b>interface-control</b> —To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1260</a></li></ul>  |



## fields (for Routing Engine Profiles)

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | fields {<br><i>field-name</i> ;<br>}   |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">routing-engine-profile</a> <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 1274</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</a> <i>profile-name</i> ],<br>[edit accounting-options <a href="#">filter-profile</a> <i>profile-name</i> ],<br>[edit accounting-options <a href="#">interface-profile</a> <i>profile-name</i> ],<br>[edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ],<br>[edit accounting-options <a href="#">routing-engine-profile</a> <i>profile-name</i> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>The [edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ] hierarchy added in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series Switches.   |
| <b>Description</b>              | Specify the accounting log file associated with the profile.   |
| <b>Options</b>                  | <i>filename</i> —Name of the log file. You must specify a filename already configured in the <b>file</b> statement at the [edit accounting-options] hierarchy level.   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1260</a></li><li>• <a href="#">Configuring the Filter Profile on page 1263</a></li><li>• <a href="#">Configuring the MIB Profile on page 1272</a></li><li>• <a href="#">Configuring the Routing Engine Profile on page 1274</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.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| <b>Description</b>              | Specify a log file to be used for accounting data.   |
| <b>Options</b>                  | <p><i>filename</i>—Name of the file in which to write accounting data.</p> <p>The remaining statements are explained separately.</p>   |
| <b>Required Privilege Level</b> | <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 Accounting-Data Log Files on page 1257</a></li> </ul>   |

## files

---

|                          |  |
|--------------------------|--|
| Syntax                   | <code>files <i>number</i>;</code>  |
| Hierarchy Level          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]  |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| Description              | Specify the maximum number of log files to be used for accounting data.  |
| Options                  | <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. |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Accounting-Data Log Files on page 1257</a></li></ul>   |

## filter-profile

---

|                          |  |
|--------------------------|--|
| Syntax                   | <pre>filter-profile <i>profile-name</i> {<br/>  <a href="#">counters</a> {<br/>    <i>counter-name</i>;<br/>  }<br/>  <a href="#">file</a> <i>filename</i>;<br/>  <a href="#">interval</a> <i>minutes</i>;<br/>}</pre>   |
| Hierarchy Level          | [edit accounting-options]  |
| Release Information      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| Description              | Create a profile to filter and collect packet and byte count statistics and write them to a file in the <b>/var/log</b> 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. |
| Options                  | <i>profile-name</i> —Name of the filter profile.<br><br>The remaining statements are explained separately.   |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Filter Profile on page 1263</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.  |
| <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>Ethernet Port Switching Feature Guide for Security Devices</i></li> <li>• <i>Layer 2 Bridging and Transparent Mode Feature Guide for Security Devices</i></li> <li>• <i>Processing Overview Feature Guide for Security Devices</i></li> <li>• <i>Junos OS Logical Systems Library for Security Devices</i></li> </ul> |

## hardware-timestamp

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | hardware-timestamp;  |
| <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 8.1.<br>Statement applied to MX Series routers in Junos OS Release 10.0.<br>Statement introduced in Junos OS Release 10.3 for EX Series switches.   |
| <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> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |

## idp (Security Alarms)

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | idp;  |
| <b>Hierarchy Level</b>          | [edit security alarms potential-violation]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.  |
| <b>Description</b>              | Configure alarms for IDP attack.  |
| <b>Required Privilege Level</b> | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>              |

## interface-profile

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>interface-profile <i>profile-name</i> {<br/>    <b>fields</b> {<br/>        <i>field-name</i>;<br/>    }<br/>    <b>file</b> <i>filename</i>;<br/>    <b>interval</b> <i>minutes</i>;<br/>}</pre>                 |
| <b>Hierarchy Level</b>          | [edit accounting-options]  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| <b>Description</b>              | Create a profile to filter and collect error and packet statistics and write them to a file in the <code>/var/log</code> directory. You can specify an interface profile for either a physical or a logical interface. |
| <b>Options</b>                  | <p><b><i>profile-name</i></b>—Name of the interface profile.</p> <p>The remaining statements are explained separately.</p>   |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Interface Profile on page 1260</a></li></ul>   |



## interval

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <code>interval <i>minutes</i>;</code>  |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">filter-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">interface-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ],<br>[edit accounting-options <a href="#">routing-engine-profile <i>profile-name</i></a> ] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>The [edit accounting-options <a href="#">mib-profile <i>profile-name</i></a> ] hierarchy level added in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Specify how often statistics are collected for the accounting profile.   |
| <b>Options</b>                  | <b><i>minutes</i></b> —Length of time between each collection of statistics.<br><b>Range:</b> 1 through 2880 minutes<br><b>Default:</b> 30 minutes   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Interface Profile on page 1260</a></li> <li>• <a href="#">Configuring the Filter Profile on page 1263</a></li> <li>• <a href="#">Configuring the MIB Profile on page 1272</a></li> <li>• <a href="#">Configuring the Routing Engine Profile on page 1274</a></li> </ul>   |

## maximum-capture-size (Datapath Debug)

---

|                          |   |
|--------------------------|---|
| Syntax                   | maximum-capture-size <i>maximum-capture-size</i> ;  |
| Hierarchy Level          | [edit security datapath-debug]  |
| Release Information      | Statement introduced in Release 10.0 of Junos OS.   |
| Description              | Specifies maximum packet capture length.  |
| Options                  | <ul style="list-style-type: none"><li>maximum-capture-size <i>maximum-capture-size</i>—Specify the maximum packet capture length.</li></ul> <p>Range: 68 through 10,000 bytes</p> |
| Required Privilege Level | security—To view this statement in the configuration.<br>security-control—To add this statement to the configuration.   |
| Related Documentation    | <ul style="list-style-type: none"><li><a href="#">System Log Messages</a></li></ul>   |

## mib-profile

---

|                          |   |
|--------------------------|---|
| Syntax                   | mib-profile <i>profile-name</i> {<br>file <i>filename</i> ;<br>interval <i>minutes</i> ;<br>object-names {<br><i>mib-object-name</i> ;<br>}<br>operation <i>operation-name</i> ;<br>} |
| Hierarchy Level          | [edit accounting-options]   |
| Release Information      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| Description              | Create a MIB profile to collect selected MIB statistics and write them to a file in the <i>/var/log</i> directory.  |
| Options                  | <i>profile-name</i> —Name of the MIB statistics profile.<br><br>The remaining statements are explained separately.  |
| Required Privilege Level | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| Related Documentation    | <ul style="list-style-type: none"><li><a href="#">Configuring the MIB Profile on page 1272</a></li></ul>  |

## mpls (Security Forwarding Options)

|                            |   |
|----------------------------|---|
| <b>Syntax</b>              | <code>mpls {<br/>    mode packet-based;<br/>}</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.<br>security-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>MPLS Feature Guide for Security Devices</i></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.<br>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 1342</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>              | For J Series Services Routers only. Store log files used for accounting data in the <b>mfs/var/log</b> directory (located on DRAM) instead of the <b>cf/var/log</b> directory (located on the compact flash drive). This feature is useful for minimizing read/write traffic on the router's compact flash drive. |
|                                 | <div>  <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> </div>                                  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Storage Location of the File on page 1258</a></li> </ul>   |

## object-names

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | object-names {<br><i>mib-object-name</i> ;<br>}   |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.             |
| <b>Options</b>                  | <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.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the MIB Profile on page 1272</a></li> </ul>            |

## operation

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <code>operation operation-name;</code>   |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">mib-profile</a> <i>profile-name</i> ]   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| <b>Description</b>              | Specify the name of the operation used to collect MIB statistics for an accounting-data log file.  |
| <b>Options</b>                  | <b><i>operation-name</i></b> —Name of the operation to use. You can specify a <b>get</b> , <b>get-next</b> , or <b>walk</b> operation.<br><b>Default:</b> walk |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the MIB Profile on page 1272</a></li></ul>   |

## packet-capture

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>packet-capture {<br/>  disable;<br/>  file <i>filename</i> &lt;files <i>number</i>&gt; &lt;size <i>bytes</i>&gt; &lt;world-readable   no-world-readable&gt;;<br/>  maximum-capture-size <i>number</i>;<br/>}</pre>  |
| <b>Hierarchy Level</b>          | [edit forwarding-options]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.  |
| <b>Description</b>              | Configure packet capture on a device.  |
| <b>Options</b>                  | <p><b>disable</b>—Disable packet capture on the router.</p> <p><b>file <i>filename</i></b>—Name of the file to enable packet capture.</p> <ul style="list-style-type: none"><li>• <i>number</i>—Maximum size of file.</li><li>• <i>no-world-readable</i>—Restrict file access to the owner.</li><li>• <i>world-readable</i>—Enable unrestricted file access.</li></ul> <p><b>maximum-capture-size</b>—Configure the maximum size of capture for packets.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Packet Capture Overview on page 1246</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>• <i>[edit security flow] Hierarchy Level</i></li> <li>• <i>Flow-Based Processing Feature Guide for Security Devices</i></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],<br>[edit services rpm probe <i>owner</i> test <i>test-name</i> ]                                 |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>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.<br>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.<br>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.<br><b>Default:</b> 100.   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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],<br>[edit services rpm probe <i>owner</i> test <i>test-name</i> ]  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>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.<br>interface-control—To add this statement to the configuration.  |

## routing-engine-profile

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>routing-engine-profile <i>profile-name</i> {<br/>    <b>fields</b> {<br/>        <i>field-name</i>;<br/>    }<br/>    <b>file</b> <i>filename</i>;<br/>    <b>interval</b> <i>minutes</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit accounting-options]   |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.   |
| <b>Description</b>              | Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the <code>/var/log</code> directory.  |
| <b>Options</b>                  | <p><b><i>profile-name</i></b>—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 1274</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.  |
| <b>Required Privilege Level</b> | services—To view this statement in the configuration.<br>services-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>IP Monitoring Feature Guide for Security Devices</i></li></ul>             |

## size

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <code>size bytes;</code>   |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.  |
| <b>Description</b>              | Specify attributes of an accounting-data log file.   |
| <b>Options</b>                  | <p><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.</p> <p><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</p> <p><b>Range:</b> 256 KB through 1 GB</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Maximum Size of the File on page 1259</a></li> </ul>  |

## source-classes

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>source-classes {     source-class-name; }</pre>  |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">class-usage-profile</a> <i>profile-name</i> ]  |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| <b>Description</b>              | Specify the source classes for which statistics are collected.  |
| <b>Options</b>                  | <b>source-class-name</b> —Name of the source class to include in the class usage profile.                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring a Class Usage Profile on page 1270</a></li> </ul>        |

## start-time

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <code>start-time <i>time</i>;</code>  |
| <b>Hierarchy Level</b>          | [edit accounting-options <a href="#">file</a> <i>filename</i> ]   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 8.2.<br>Statement introduced in Junos OS Release 9.0 for EX Series switches.       |
| <b>Description</b>              | Specify the start time for transfer of an accounting-data log file.   |
| <b>Options</b>                  | <i>time</i> —Start time for file transfer.<br><b>Syntax:</b> <i>YYYY-MM-DD.hh:mm</i>  |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Start Time for File Transfer on page 1259</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.<br>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>                  | <i>url url</i> —For HTTP probe types, specify a fully formed URL that includes <b>http://</b> in the URL address.<br><br><i>address address</i> —For all other probe types, specify an IPv4 address for the target host. |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>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.<br>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.<br/>Default: 1</li> <li>• <b>total-loss</b>—Measures total probe loss count indicating test failure, from 0 through 15.<br/>Default: 1</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>   |

## traceoptions (Security Datapath Debug)

```
Syntax  traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        no-remote-trace;
    }
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Command introduced in Junos OS Release 9.6.

**Description** Sets the trace options for datapath-debug.

**Options** • **file**—Configure the trace file options.

- **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.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

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). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the 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 file size, you also must specify a maximum number of trace files with the files 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
- **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** • *IDP Monitoring and Troubleshooting Guide for Security Devices*

## 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 1259](#)

## 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.<br>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> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |

## Administration

---

- [Monitoring Security Devices on page 1355](#)
- [Alarms on page 1477](#)

- [Data Path Debugging and Trace Options on page 1479](#)
- [MPLS on page 1485](#)
- [Packet Capture on page 1499](#)
- [RPM on page 1507](#)
- [Operational Commands on page 1511](#)

## Monitoring Security Devices

- [Displaying Multicast Path Information on page 1356](#)
- [Displaying Real-Time Interface Information on page 1358](#)
- [Displaying Real-Time Monitoring Information on page 1360](#)
- [Monitoring Address Pools on page 1362](#)
- [Monitoring Antivirus Scan Engine Status on page 1363](#)
- [Monitoring Antivirus Scan Results on page 1364](#)
- [Monitoring Antivirus Session Status on page 1366](#)
- [Monitoring Class-of-Service Performance on page 1367](#)
- [Monitoring Content Filtering Configurations on page 1374](#)
- [Monitoring CoS Classifiers on page 1375](#)
- [Monitoring DHCP Client Bindings on page 1376](#)
- [Monitoring Ethernet Switching on page 1377](#)
- [Monitoring Events on page 1378](#)
- [Monitoring GVRP on page 1380](#)
- [Monitoring H.323 ALG Information on page 1381](#)
- [Monitoring Interfaces on page 1382](#)
- [Monitoring MGCP ALGs on page 1384](#)
- [Monitoring MPLS Traffic Engineering Information on page 1387](#)
- [Monitoring NAT on page 1392](#)
- [Monitoring Policy Statistics on page 1402](#)
- [Monitoring PPP on page 1403](#)
- [Monitoring PPPoE on page 1404](#)
- [Monitoring Reports on page 1407](#)
- [Monitoring Routing Information on page 1413](#)
- [Monitoring SCCP ALGs on page 1421](#)
- [Monitoring Security Events by Policy on page 1423](#)
- [Monitoring Security Features on page 1425](#)
- [Monitoring SIP ALGs on page 1439](#)
- [Monitoring Spanning Tree on page 1443](#)
- [Monitoring the System on page 1444](#)
- [Monitoring Voice ALG H.323 on page 1452](#)

- [Monitoring Voice ALG MGCP on page 1454](#)
- [Monitoring Voice ALG SCCP on page 1457](#)
- [Monitoring Voice ALG SIP on page 1460](#)
- [Monitoring Voice ALG Summary on page 1465](#)
- [Monitoring VPNs on page 1466](#)
- [Monitoring the WAN Acceleration Interface on page 1476](#)
- [Monitoring Web Filtering Configurations on page 1476](#)

### Displaying Multicast Path Information

To display information about a multicast path from a source to the J Series 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 133 on page 1356](#) describes the **mtrace from-source** command options.

**Table 133: 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 J Series 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 133: 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 134 on page 1357 summarizes the output fields of the display.



**NOTE:** The packet statistics gathered from Juniper Networks devices and routing nodes always display as 0.

Table 134: 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 134: 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.  |

### 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 135 on page 1358](#) and [Table 136 on page 1359](#) list the keys you use to control the display using the ***interface-name*** and **traffic** options. (The keys are not case sensitive.)

Table 135: 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.   |



Table 135: CLI monitor interface Output Control Keys (*continued*)

| Key      | Action   |
|----------|--|
| 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 136: CLI monitor interface traffic Output Control Keys

| Key      | Action  |
|----------|---|
| b        | Displays the statistics in units of bytes and bytes per second (bps).   |
| c        | Clears (returns to 0) the delta counters in the <b>Delta</b> column. The statistics counters are not cleared. |
| d        | Displays the <b>Delta</b> column instead of the rate column—in bps or packets per second (pps).               |
| p        | Displays the statistics in units of packets and packets per second (pps).                                     |
| q or ESC | Quits the command and returns to the command prompt.  |
| r        | Displays the rate column—in bps and pps—instead of the <b>Delta</b> column.                                   |

The following are sample displays from the **monitor interface** command:

```
user@host> monitor interface fe-0/0/0
```

```

host1                               Seconds: 5                               Time: 04:38:40
                                      Delay: 3/0/10

Interface: fe-0/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 1000mbps
Traffic statistics:
  Input bytes:      885405423 (3248 bps)
  Output bytes:    137411893 (3344 bps)
  Input packets:   7155064 (2 pps)
  Output packets:  636071 (1 pps)
Error statistics:
  Input errors:    0
  Input drops:    0
  Input framing errors: 0
  Policed discards: 0
  L3 incompletes: 0
  L2 channel errors: 0
  L2 mismatch timeouts: 0
Current delta
[2631]
[10243]
[28]
[23]
[0]
[0]
[0]
[0]
[0]
[0]
[0]
[0]
```

```

Carrier transitions:          1          [0]
Output errors:               0          [0]
Output drops:               0          [0]
Aged packets:               0          [0]
Active alarms : None
Active defects: None
Input MAC/Filter statistics:
  Unicast packets           73083       [16]
  Broadcast packets        3629058     [5]
  Multicast packets        3511364     [3]
  Oversized frames         0          [0]
  Packet reject count      0          [0]
  DA rejects               0          [0]
  SA rejects               0          [0]
Output MAC/Filter Statistics:
  Unicast packets          629555      [28]
  Broadcast packets        6494
  Multicast packet         [0]

```



**NOTE:** The output fields that display when you enter the `monitor interface interface-name` command are determined by the interface you specify.

```
user@host> monitor interface traffic
```

| Interface | Link | Input packets | (pps)   | Output packets | (pps)   |
|-----------|------|---------------|---------|----------------|---------|
| fe-0/0/0  | Up   | 42334         | (5)     | 23306          | (3)     |
| fe-0/0/1  | Up   | 587525876     | (12252) | 589621478      | (12891) |

#### Related Documentation

- [Junos OS Interfaces Library for Security Devices](#)

### Displaying Real-Time Monitoring Information

To display real-time monitoring information about each device between the J Series 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 137 on page 1360 describes the **traceroute monitor** command options.

**Table 137: CLI traceroute monitor Command Options**

| Option                  | Description   |
|-------------------------|---|
| <i>host</i>             | Sends traceroute packets to the hostname or IP address you specify.   |
| <i>count number</i>     | (Optional) Limits the number of ping requests, in packets, to send in summary mode. If you do not specify a count, ping requests are continuously sent until you press Q. |
| <i>inet</i>             | (Optional) Forces the traceroute packets to an IPv4 destination.  |
| <i>inet6</i>            | (Optional) Forces the traceroute packets to an IPv6 destination.  |
| <i>interval seconds</i> | (Optional) Sets the interval between ping requests, in seconds. The default value is 1 second.  |

Table 137: CLI traceroute monitor Command Options (*continued*)

| Option                | Description  |
|-----------------------|--|
| <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          0.0%    5
9.4  8.6   4.8   9.9   2.1
2. 173.24.232.66          0.0%    5
7.9 17.2   7.9  29.4  11.0
3. 173.24.232.66          0.0%    5
9.9  9.3   8.7   9.9   0.5
4. 173.24.232.66          0.0%    5
9.9  9.8   9.5  10.0   0.2

```

Table 138 on page 1361 summarizes the output fields of the display.

Table 138: CLI traceroute monitor Command Output Summary

| Field               | Description  |
|---------------------|--|
| <b>host</b>         | Hostname or IP address of the J Series device issuing the <b>traceroute monitor</b> command. |
| <b>psizesize</b>    | Size of ping request packet, in bytes.   |
| <b>Keys</b>         |  |
| <b>Help</b>         | Displays the Help for the CLI commands.<br>Press H to display the Help.                      |
| <b>Display mode</b> | Toggles the display mode.<br>Press D to toggle the display mode                              |

Table 138: CLI traceroute monitor Command Output Summary (*continued*)

| Field                     | Description   |
|---------------------------|---|
| <b>Restart statistics</b> | Restarts the <b>traceroute monitor</b> command.<br><br>Press R to restart the <b>traceroute monitor</b> command.        |
| <b>Order of fields</b>    | Sets the order of the displayed fields.<br><br>Press O to set the order of the displayed fields.                        |
| <b>quit</b>               | Quits the <b>traceroute monitor</b> command.<br><br>Press Q to quit the <b>traceroute monitor</b> command.              |
| <b>Packets</b>            |   |
| <i>number</i>             | Number of the hop (device) along the route to the final destination host.   |
| <b>Host</b>               | Hostname or IP address of the device at each hop.   |
| <b>Loss%</b>              | Percent of packet loss. The number of ping responses divided by the number of ping requests, specified as a percentage. |
| <b>Pings</b>              |   |
| <b>Snt</b>                | Number of ping requests sent to the device at this hop.   |
| <b>Last</b>               | Most recent round-trip time, in milliseconds, to the device at this hop.  |
| <b>Avg</b>                | Average round-trip time, in milliseconds, to the device at this hop.  |
| <b>Best</b>               | Shortest round-trip time, in milliseconds, to the device at this hop.   |
| <b>Wrst</b>               | Longest round-trip time, in milliseconds, to the device at this hop.  |
| <b>StDev</b>              | Standard deviation of round-trip times, in milliseconds, to the device at this hop.                                     |

### 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 139 on page 1362](#) summarizes key output fields in the Address Pools page.

Table 139: Address Pools Monitoring Page

| Field                          | Values | Additional Information |
|--------------------------------|--------|------------------------|
| <b>Address Pool Properties</b> |        |                        |

Table 139: Address Pools Monitoring Page (*continued*)

| Field                                  | Values  | Additional Information   |
|--|---|--|
| 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.                        | -  |
| 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 1382](#)
  - [Threats Monitoring Report on page 1407](#)

### 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

- *UTM Full Antivirus Protection Feature Guide for Security Devices*
- *Full Antivirus Configuration Overview*
- [Monitoring Antivirus Session Status on page 1366](#)
- [Monitoring Antivirus Scan Results on page 1364](#)

---

### 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**

- [UTM Full Antivirus Protection Feature Guide for Security Devices](#)
- [Monitoring Antivirus Session Status on page 1366](#)

---

### 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**

- *UTM Full Antivirus Protection Feature Guide for Security Devices*
- *Full Antivirus Configuration Overview*
- [Monitoring Antivirus Scan Engine Status on page 1363](#)
- [Monitoring Antivirus Scan Results on page 1364](#)

---

### 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 1367](#)
- [Monitoring CoS Classifiers on page 1368](#)
- [Monitoring CoS Value Aliases on page 1369](#)
- [Monitoring CoS RED Drop Profiles on page 1370](#)
- [Monitoring CoS Forwarding Classes on page 1371](#)
- [Monitoring CoS Rewrite Rules on page 1372](#)
- [Monitoring CoS Scheduler Maps on page 1373](#)

#### *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 140 on page 1368](#) summarizes key output fields for CoS interfaces.

Table 140: 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 (+). |
| 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 141 on page 1368](#) summarizes key output fields for CoS classifiers.

Table 141: Summary of Key CoS Classifier Output Fields

|                 |                       |   |
|-----------------|-----------------------|---|
| Classifier Name | Name of a classifier. | To display classifier assignments, click the plus sign (+). |
|-----------------|-----------------------|---|

Table 141: Summary of Key CoS Classifier Output Fields (*continued*)

|                            |  |
|----------------------------|--|
| CoS Value Type             | <p>The classifiers are displayed by type:</p> <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.   |

**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 142 on page 1370](#) summarizes key output fields for CoS value aliases.

Table 142: 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 143 on page 1370](#) summarizes key output fields for CoS RED drop profiles.

Table 143: Summary of Key CoS RED Drop Profile Output Fields

| Field                 | Values  | Additional Information   |
|-----------------------|---|--|
| RED Drop Profile Name | Name of the RED drop profile.<br><br>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. |

Table 143: Summary of Key CoS RED Drop Profile Output Fields (*continued*)

| Field            | Values   | Additional Information |
|------------------|--|------------------------|
| 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 144 on page 1372](#) summarizes key output fields for CoS forwarding classes.

Table 144: 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 145 on page 1372 summarizes key output fields for CoS rewrite rules.

Table 145: 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 145: 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 146 on page 1373 summarizes key output fields for CoS scheduler maps.

Table 146: 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 146: 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### Monitoring Content Filtering Configurations

**Purpose** View content filtering statistics.



**Action** To view content filtering statistics in the CLI, enter the `user@host > show security utm content-filtering statistics` command.

The content filtering **show statistics** command displays the following information:

```
Base on command list: # Blocked
Base on mime list: # Blocked
Base on extension list: # Blocked
ActiveX plugin: # Blocked
Java applet: # Blocked
EXE files: # Blocked
ZIP files: # Blocked
HTTP cookie: # Blocked
```

To view content filtering statistics using J-Web:

1. Select **Clear Content filtering statistics** **Monitor>Security>UTM>Content Filtering** **Monitor>Security>UTM>Content Filtering**.

The following statistics become viewable in the right pane.

```
Base on command list: # Passed # Blocked
Base on mime list: # Passed # Blocked
Base on extension list: # Passed # Blocked
ActiveX plugin: # Passed # Blocked
Java applet: # Passed # Blocked
EXE files: # Passed # Blocked
ZIP files: # Passed # Blocked
HTTP cookie: # Passed # Blocked
```

2. You can click **Clear Content filtering statistics** to clear all current viewable statistics and begin collecting new statistics.

#### Related Documentation

- *UTM Content Filtering Feature Guide for Security Devices*
- *Content Filtering Overview*
- *Understanding Content Filtering Protocol Support*
- *Content Filtering Configuration Overview*
- *Example: Attaching Content Filtering UTM Policies to Security Policies*

### 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 141 on page 1368](#) summarizes key output fields for CoS classifiers.

**Table 147: Summary of Key CoS Classifier Output Fields**

| Classifier Name | Name of a classifier. | To display classifier assignments, click the plus sign (+). |
|-----------------|-----------------------|---|
|-----------------|-----------------------|---|

Table 147: Summary of Key CoS Classifier Output Fields (*continued*)

|                            |  |
|----------------------------|--|
| CoS Value Type             | <p>The classifiers are displayed by type:</p> <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 1367](#)
- [Monitoring CoS Value Aliases on page 1369](#)
- [Monitoring CoS RED Drop Profiles on page 1370](#)
- [Monitoring CoS Forwarding Classes on page 1371](#)
- [Monitoring CoS Rewrite Rules on page 1372](#)
- [Monitoring CoS Scheduler Maps on page 1373](#)

### 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 148 on page 1377](#) summarizes the key output fields in the DHCP client binding displays.

Table 148: 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 1404](#)
  - [Understanding DHCP Client Operation on page 687](#)

### 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 149 on page 1377](#) summarizes the Ethernet Switching output fields.

Table 149: 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.   |                        |

Table 149: Summary of Ethernet Switching Output Fields (*continued*)

| Field       | Values  | Additional Information |
|-------------|---|------------------------|
| Interfaces  | Interface associated with learned MAC addresses or All-members (flood entry). |                        |
| VLAN-ID     | The VLAN ID.  |                        |
| MAC Address | The learned MAC address.  |                        |
| Time        | Timestamp when the MAC address was added or deleted from the log.             |                        |
| State       | Indicates the MAC address learned on the interface.                           |                        |

- Related Documentation**
- [Monitoring Overview on page 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### 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 150 on page 1379](#) summarizes key output fields in the events page.

Table 150: 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.                       | —                      |
| 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.                             | —                      |

Table 150: Events Monitoring Page (*continued*)

| Field             | Value  | Additional Information |
|-------------------|--|------------------------|
| 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          | <p>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.</p>   | —                      |
| Event Description | <p>Displays a more detailed explanation of the message.</p>  | —                      |
| Time              | <p>Time that the error or event occurred.</p>  | —                      |

- Related Documentation**
- [Monitoring Alarms on page 1478](#)
  - [Monitoring Security Events by Policy on page 1423](#)

### 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 151 on page 1381](#) summarizes key output fields in the GVRP page.

Table 151: 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.  | —                      |
| Protocol Status                  | Displays whether GVRP is enabled or disabled.   | —                      |

- Related Documentation**
- [Monitoring Ethernet Switching on page 1377](#)
  - [Monitoring Spanning Tree on page 1443](#)

### [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 152 on page 1381](#) summarizes key output fields in the H.323 counters display.

Table 152: 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. | —                      |

Table 152: Summary of Key H.323 Counters Output Fields (*continued*)

| Field                       | Values   | Additional Information  |
|-----------------------------|--|---|
| 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.   | —   |
| 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)

### 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 1231](#)
- [Monitoring Address Pools on page 1362](#)
- *Junos OS Interfaces Library for Security Devices*

### Monitoring MGCP ALGs

This section contains the following topics:

- [Monitoring MGCP ALG Calls on page 1384](#)
- [Monitoring MGCP ALG Counters on page 1385](#)
- [Monitoring MGCP ALG Endpoints on page 1386](#)

#### 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 153 on page 1384](#) summarizes key output fields in the MGCP calls display.

**Table 153: Summary of Key MGCP Calls Output Fields**

| Field                          | Values   | Additional Information |
|--------------------------------|--|------------------------|
| <b>MGCP Calls Information</b>  |  |                        |
| Endpoint@GW                    | Endpoint name.   | —                      |
| Zone                           | <ul style="list-style-type: none"> <li>• <b>trust</b>—Trust zone.</li> <li>• <b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| Call ID                        | Call identifier for ALG MGCP.  | —                      |
| RM Group                       | Resource manager group ID.   | —                      |
| Call Duration                  | Duration for which connection is active.   | —                      |
| Connection Id                  | Connection identifier for MGCP ALG calls.  | —                      |
| <b>Calls Details: Endpoint</b> |  |                        |
| Local SDP                      | IP address of the MGCP ALG local call owner, as per the Session Description Protocol (SDP).                          | —                      |

Table 153: Summary of Key MGCP Calls Output Fields (*continued*)

| Field      | Values  | Additional Information |
|------------|---|------------------------|
| 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 154 on page 1385 summarizes key output fields in the MGCP counters display.

Table 154: 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.    | —                      |
| <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.               | —                      |

Table 154: Summary of Key MGCP Counters Output Fields (*continued*)

| Field                  | Values   | Additional Information |
|------------------------|--|------------------------|
| 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 155 on page 1386](#) summarizes key output fields in the MGCP endpoints display.

Table 155: Summary of Key MGCP Endpoints Output Fields

| Field                          | Values   | Additional Information |
|--------------------------------|--|------------------------|
| <b>MGCP Endpoints</b>          |  |                        |
| Gateway                        | IP address of the gateway.   | —                      |
| Zone                           | <ul style="list-style-type: none"> <li><b>trust</b>—Trust zone.</li> <li><b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| IP                             | IP address.  | —                      |
| <b>Endpoints: Gateway name</b> |  |                        |
| Endpoint                       | Endpoint name.   | —                      |
| Transaction #                  | Transaction identifier.  | —                      |
| Call #                         | Call identifier.   | —                      |
| Notified Entity                | The certificate authority (CA) currently controlling the gateway.  | —                      |

- Related Documentation**
- [Monitoring Overview on page 1231](#)
  - [Monitoring Interfaces on page 1382](#)

### Monitoring MPLS Traffic Engineering Information

This section contains the following topics:

- [Monitoring MPLS Interfaces on page 1387](#)
- [Monitoring MPLS LSP Information on page 1387](#)
- [Monitoring MPLS LSP Statistics on page 1388](#)
- [Monitoring RSVP Session Information on page 1389](#)
- [Monitoring MPLS RSVP Interfaces Information on page 1391](#)

#### 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 156 on page 1387](#) summarizes key output fields in the MPLS interface information display.

**Table 156: 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 157 on page 1388](#) summarizes key output fields in the MPLS LSP information display.

Table 157: 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.  |
| 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 158 on page 1389 summarizes key output fields in the MPLS LSP statistics display.

**Table 158: Summary of Key MPLS LSP Statistics Output Fields**

| Field       | Values  | Additional Information   |
|-------------|---|--|
| Ingress LSP | Information about LSPs on the inbound device. Each session has one line of output.  | —  |
| Egress LSP  | Information about the LSPs on the outbound device. Each session has one line of output.   | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| Transit LSP | Number of LSPs on the transit routers and the state of these paths.   | MPLS learns this information by querying RSVP, which holds all the transit and outbound session information. |
| To          | Destination (outbound device) of the session.   | —  |
| From        | Source (inbound device) of the session.   | —  |
| State       | State of the path: <b>Up</b> , <b>Down</b> , or <b>AdminDn</b> .  | <b>AdminDn</b> indicates that the LSP is being taken down gracefully.  |
| Packets     | Total number of packets received on the LSP from the upstream neighbor.   | —  |
| Bytes       | Total number of bytes received on the LSP from the upstream neighbor.   | —  |
| LSPname     | Configured name of the LSP.   | —  |
| Total       | Total number of LSPs displayed for the particular type— <b>ingress</b> (inbound), <b>egress</b> (outbound), or <b>transit</b> . | —  |

#### **Monitoring RSVP Session Information**

**Purpose** View information about RSVP-signaled LSP sessions currently active on the device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.

**Action** Select **Monitor>MPLS>RSVP Sessions** in the J-Web user interface, or enter the **show rsvp session** command.

[Table 159 on page 1390](#) summarizes key output fields in the RSVP session information display.

**Table 159: 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.  | –  |
| 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 160 on page 1391](#) summarizes key output fields in the RSVP interfaces information display.

**Table 160: Summary of Key RSVP Interfaces Information Output Fields**

| Field          | Values   | Additional Information |
|----------------|--|------------------------|
| RSVP Interface | Number of interfaces on which RSVP is active.<br>Each interface has one line of output.  | —                      |
| Interface      | Name of the interface.   | —                      |
| State          | State of the interface: <ul style="list-style-type: none"> <li>• <b>Disabled</b>—No traffic engineering information is displayed.</li> <li>• <b>Down</b>—The interface is not operational.</li> <li>• <b>Enabled</b>—Displays traffic engineering information.</li> <li>• <b>Up</b>—The interface is operational.</li> </ul> | —                      |
| Active resv    | Number of reservations that are actively reserving bandwidth on the interface.   | —                      |
| Subscription   | User-configured subscription factor.   | —                      |
| Static BW      | Total interface bandwidth, in bits per second (bps).   | —                      |
| Available BW   | Amount of bandwidth that RSVP is allowed to reserve, in bits per second (bps). It is equal to <b>(static bandwidth X subscription factor)</b> .  | —                      |
| Reserved BW    | Currently reserved bandwidth, in bits per second (bps).  | —                      |
| Highwater mark | Highest bandwidth that has ever been reserved on this interface, in bits per second (bps).   | —                      |

**Related Documentation**

- [Configuring Ping MPLS on page 1281](#)
- [MPLS Connection Checking Overview on page 1244](#)

- [Monitoring Overview on page 1231](#)
- [Monitoring Interfaces on page 1382](#)
- *Junos OS Interfaces Library for Security Devices*

## Monitoring NAT

This section contains the following topics:

- [Monitoring Source NAT Information on page 1392](#)
- [Monitoring Destination NAT Information on page 1398](#)
- [Monitoring Static NAT Information on page 1399](#)
- [Monitoring Incoming Table Information on page 1401](#)
- [Monitoring Interface NAT Port Information on page 1402](#)

### 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 161 on page 1392](#) describes the available options for monitoring source NAT.

**Table 161: 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.   | —   |

Table 161: Source NAT Monitoring Page (*continued*)

| Field                                  | Description   | Action  |
|--|---|---|
| Source address range                   | Source IP address range in the source pool.   | —   |
| Destination address range              | Destination IP address range in the source pool.  | —   |
| Source ports                           | Source port numbers.  | —   |
| Ip protocol                            | IP protocol.  | —   |
| Action                                 | Action taken for a packet that matches a rule.  | —   |
| Persistent NAT type                    | Persistent NAT type.  | —   |
| Inactivity timeout                     | Inactivity timeout interval for the persistent NAT binding.   | —   |
| Alarm threshold                        | Utilization alarm threshold.  |   |
| Max session number                     | The maximum number of sessions.   | —   |
| Sessions (Succ/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>Succ—Number of successful session installations after the NAT rule is matched.</li> <li>Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>Current—Number of sessions that reference the specified rule.</li> </ul> | —   |
| Translation Hits                       | Number of times a translation in the translation table is used for a source NAT rule.   | —   |
| <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.  | —   |

Table 161: Source NAT Monitoring Page (*continued*)

| Field                                  | Description  | Action |
|--|--|--------|
| Address range                          | IP address range in the source pool.   | —      |
| Single/Twin ports                      | Number of allocated single and twin ports.                                     | —      |
| Port                                   | Source port number in the pool.  | —      |
| Address assignment                     | Displays the type of address assignment.                                       | —      |
| Alarm threshold                        | Utilization alarm threshold.   | —      |
| Port overloading factor                | Port overloading capacity.   | —      |
| Routing instance                       | Name of the routing instance.  | —      |
| Total addresses                        | Total IP address, IP address set, or address book entry.                       | —      |
| Host address base                      | Host base address of the original source IP address range.                     | —      |
| Translation hits                       | Number of times a translation in the translation table is used for source NAT. | —      |
| <b>Top 10 Translation Hits</b>         |  |        |
| Graph                                  | Displays the graph of top 10 translation hits.                                 | —      |
| <b>Persistent NAT</b>                  |  |        |
| <b>Persistent NAT table statistics</b> |  |        |
| binding total                          | Displays the total number of persistent NAT bindings for the FPC.              | —      |
| 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>            |  |        |

Table 161: Source NAT Monitoring Page (*continued*)

| Field                               | Description   | Action   |
|-------------------------------------|---|--|
| Source NAT pool                     | Name of the pool.   | Select all pools or a specific pool to display from the list.              |
| Internal IP                         | Internal IP address.  | Select all IP addresses or a specific IP address to display from the list. |
| Internal port                       | Displays the internal ports configured in the system.   | Select the port to display from the list.                                  |
| Internal protocol                   | Internal protocols .  | Select all protocols or a specific protocol to display from the list.      |
| Internal IP                         | Internal transport IP address of the outgoing session from internal to external.                          | —  |
| Internal port                       | Internal transport port number of the outgoing session from internal to external.                         | —  |
| Internal protocol                   | Internal protocol of the outgoing session from internal to external.                                      | —  |
| Reflective IP                       | Translated IP address of the source IP address.   | —  |
| Reflective port                     | Displays the translated number of the port.   | —  |
| Reflective protocol                 | Translated protocol.  | —  |
| Source NAT pool                     | Name of the source NAT pool where persistent NAT is used.   | —  |
| Type                                | Persistent NAT type.  | —  |
| Left time/Conf time                 | Inactivity timeout period that remains and the configured timeout value.                                  | —  |
| 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.                                 | —  |

---

**External node table**


---

Table 161: Source NAT Monitoring Page (*continued*)

| Field                                   | Description  | Action  |
|---|--|---|
| Internal IP                             | Internal transport IP address of the outgoing session from internal to external. | —   |
| Internal port                           | Internal port number of the outgoing session from internal to external.          | —   |
| External IP                             | External IP address of the outgoing session from internal to external.           | —   |
| External port                           | External port of the outgoing session from internal to external.                 | —   |
| Zone                                    | External zone of the outgoing session from internal to external.                 | —   |
| <b>Paired Address</b>                   |  |   |
| Pool name                               | Name of the pool.  | Select all pools or a specific pool to display from the list.   |
| Specified Address                       | IP address.  | Select all addresses, or select the internal or external IP address to display, and enter the IP address.   |
| Pool name                               | Displays the selected pool or pools.   | —   |
| Internal address                        | Displays the internal IP address.  | —   |
| External address                        | Displays the external IP address.  | —   |
| <b>Resource Usage</b>                   |  |   |
| <b>Utilization for all source pools</b> |  |   |
| Pool name                               | Name of the pool.  | To view additional usage information for Port Address Translation (PAT) pools, select a pool name. The information displays under Detail Port Utilization for Specified Pool. |
| Pool type                               | Pool type: PAT or Non-PAT.   | —   |
| Port overloading factor                 | Port overloading capacity for PAT pools.   | —   |
| Address                                 | Addresses in the pool.   | —   |

Table 161: Source NAT Monitoring Page (*continued*)

| Field   | Description   | Action  |
|---|---|---|
| Used  | <p>Number of used resources in the pool.</p> <p>For Non-PAT pools, the number of used IP addresses is displayed.</p> <p>For PAT pools, the number of used ports is displayed.</p>   | —   |
| Available   | <p>Number of available resources in the pool.</p> <p>For Non-PAT pools, the number of available IP addresses is displayed.</p> <p>For PAT pools, the number of available ports is displayed.</p>  | —   |
| Total   | <p>Number of used and available resources in the pool.</p> <p>For Non-PAT pools, the total number of used and available IP addresses is displayed.</p> <p>For PAT pools, the total number of used and available ports is displayed.</p> | —   |
| Usage   | <p>Percent of resources used.</p> <p>For Non-PAT pools, the percent of IP addresses used is displayed.</p> <p>For PAT pools, the percent of ports, including single and twin ports, is displayed.</p>                                   | —   |
| 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 162 on page 1398](#) summarizes key output fields in the destination NAT display.

**Table 162: 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 162: Summary of Key Destination NAT Output Fields (*continued*)

| Field                                  | Values  | Action  |
|--|---|---|
| Sessions (Succ/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>Succ—Number of successful session installations after the NAT rule is matched.</li> <li>Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>Current—Number of sessions that reference the specified rule.</li> </ul> | —   |
| Translation hits                       | Number of times a translation in the translation table is used for a destination NAT rule.  | —   |
| <b>Pools</b>                           |   |   |
| Pool Name                              | The names of the pools.   | Select all pools or a specific pool to display from the list. |
| Total Pools                            | Total pools added.  | —   |
| ID                                     | ID of the pool.   | —   |
| Name                                   | Name of the destination pool.   | —   |
| Address range                          | IP address range in the destination pool.   | —   |
| Port                                   | Destination port number in the pool.  | —   |
| Routing instance                       | Name of the routing instance.   | —   |
| Total addresses                        | Total IP address, IP address set, or address book entry.  | —   |
| Translation hits                       | Number of times a translation in the translation table is used for destination NAT.   | —   |
| <b>Top 10 Translation Hits</b>         |   |   |
| Graph                                  | Displays the graph of top 10 translation hits.  | —   |

**Monitoring Static NAT Information**

**Purpose** View static NAT rule information.

**Action** Select **Monitor>NAT>Static NAT** in the J-Web user interface, or enter the following CLI command:

**show security nat static rule**

Table 163 on page 1400 summarizes key output fields in the static NAT display.

**Table 163: 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/<br>Failed/<br>Current) | Successful, failed, and current sessions. <ul style="list-style-type: none"> <li>• Succ—Number of successful session installations after the NAT rule is matched.</li> <li>• Failed—Number of unsuccessful session installations after the NAT rule is matched.</li> <li>• Current—Number of sessions that reference the specified rule.</li> </ul> | —   |

Table 163: 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 164 on page 1401](#) summarizes key output fields in the incoming table display.

Table 164: 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 165 on page 1402 summarizes key output fields in the interface NAT display.

**Table 165: 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

**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 the number of packets, bytes, and sessions that enter the firewall 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 1625*
- *Checking a Security Policy Commit Failure on page 1626*
- *Verifying a Security Policy Commit on page 1626*
- *Debugging Policy Lookup on page 1627*
- *Security Policies Feature Guide for Security Devices*

### 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 1231*

- [Monitoring Interfaces on page 1382](#)
- *Junos OS Interfaces Library for Security Devices*

### 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 166 on page 1404](#) summarizes key output fields in PPPoE displays.

**Table 166: 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.   | —   |
| 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. | —   |

Table 166: Summary of Key PPPoE Output Fields (*continued*)

| Field                   | Values   | Additional Information |
|-------------------------|--|------------------------|
| 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.  | —                      |
| Received                | Number of the specific type of packet received by the PPPoE client.  | —                      |

Table 166: Summary of Key PPPoE Output Fields (*continued*)

| Field                         | Values   | Additional Information  |
|-------------------------------|--|---|
| Timeout                       | Information about the timeouts that occurred during the PPPoE session. <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 1231](#)
- [Monitoring Interfaces on page 1382](#)
- [Monitoring DHCP Client Bindings on page 1376](#)
- *Junos OS Interfaces Library for Security Devices*

### 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 1407](#)
- [Traffic Monitoring Report on page 1412](#)

#### 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 167 on page 1407](#) for a description of the page content.
  - **Activities** tab. See [Table 168 on page 1410](#) for a description of the page content.

**Table 167: Statistics Tab Output in the Threats Report**

| Field                   | Description |
|-------------------------|-------------|
| General Statistics Pane |             |

Table 167: Statistics Tab Output in the Threats Report (*continued*)

| Field                                     | Description   |
|---|---|
| Threat Category                           | One of the following categories of threats: <ul style="list-style-type: none"> <li>• Traffic</li> <li>• IDP</li> <li>• Content Security <ul style="list-style-type: none"> <li>• Antivirus</li> <li>• Antispam</li> <li>• Web Filter—Click the Web filter category to display counters for 39 subcategories.</li> <li>• Content Filter</li> </ul> </li> <li>• Firewall Event</li> </ul> |
| Severity                                  | Severity level of the threat: <ul style="list-style-type: none"> <li>• emerg</li> <li>• alert</li> <li>• crit</li> <li>• err</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• debug</li> </ul>   |
| Hits in past 24 hours                     | Number of threats encountered per category in the past 24 hours.  |
| Hits in current hour                      | Number of threats encountered per category in the last hour.  |
| <b>Threat Counts in the Past 24 Hours</b> |   |
| By Severity                               | Graph representing the number of threats received each hour for the past 24 hours sorted by severity level.   |
| By Category                               | Graph representing the number of threats received each hour for the past 24 hours sorted by category.   |
| 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.   |

Table 167: Statistics Tab Output in the Threats Report (*continued*)

| Field                                | Description   |
|--------------------------------------|---|
| Category                             | Category of each threat: <ul style="list-style-type: none"> <li>• Traffic</li> <li>• IDP</li> <li>• Content Security <ul style="list-style-type: none"> <li>• Antivirus</li> <li>• Antispam</li> <li>• Web Filter</li> <li>• Content Filter</li> </ul> </li> <li>• Firewall Event</li> </ul>  |
| Source IP/Port                       | Source IP address (and port number, if applicable) of the threat.   |
| Destination IP/Port                  | Destination IP address (and port number, if applicable) of the threat.  |
| Protocol                             | Protocol name of the threat.  |
| Description                          | Threat identification based on the category type: <ul style="list-style-type: none"> <li>• Antivirus—URL</li> <li>• Web filter—category</li> <li>• Content filter—reason</li> <li>• Antispam—sender e-mail</li> </ul>   |
| Action                               | Action taken in response to the threat.   |
| Hit Time                             | Time the threat occurred.   |
| <b>Threat Trend in past 24 hours</b> |   |
| 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.   |

Table 167: Statistics Tab Output in the Threats Report (*continued*)

| Field                | Description   |
|----------------------|---|
| Hits in current hour | Number of threats per subcategory in the last hour. |

Table 168: 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.  |
| 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.   |

Table 168: Activities Tab Output in the Threats Report (*continued*)

| Field                                | Function  |
|--------------------------------------|---|
| 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                               |   |
| 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.  |

Table 168: Activities Tab Output in the Threats Report (*continued*)

| Field          | Function                                |
|----------------|---|
| 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 169 on page 1412](#) for a description of the report.

Table 169: 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.  |
| 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.  |

Table 169: Traffic Report Output (*continued*)

| Field                            | Description   |
|----------------------------------|---|
| 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### Monitoring Routing Information

This section contains the following topics:

- [Monitoring Route Information on page 1414](#)
- [Monitoring RIP Routing Information on page 1416](#)
- [Monitoring OSPF Routing Information on page 1417](#)
- [Monitoring BGP Routing Information on page 1419](#)

**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 170 on page 1414 describes the different filters, their functions, and the associated actions.

Table 171 on page 1415 summarizes key output fields in the routing information display.

**Table 170: 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. |



Table 170: Filtering Route Messages (*continued*)

| Field         | Function   | Your Action   |
|---------------|--|---|
| 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 171: 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>I—IGP.</li> <li>E—EGP.</li> <li>?—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 172 on page 1416](#) summarizes key output fields in the RIP routing display in the J-Web user interface.

**Table 172: 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.  |

Table 172: Summary of Key RIP Routing Output Fields (*continued*)

| Field        | Values  | Additional Information |
|--------------|---|------------------------|
| 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 173 on page 1417](#) summarizes key output fields in the OSPF routing display in the J-Web user interface.

Table 173: 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> |   |   |

Table 173: Summary of Key OSPF Routing Output Fields (*continued*)

| Field                    | Values  | Additional Information   |
|--------------------------|---|--|
| <b>Packets tab</b>       |   |  |
| Sent                     | Displays the total number of packets sent.  | —  |
| Received                 | Displays the total number of packets received.  | —  |
| <b>Details tab</b>       |   |  |
| Flood Queue Depth        | Number of entries in the extended queue.  | —  |
| Total Retransmits        | Number of retransmission entries enqueued.  | —  |
| Total Database Summaries | Total number of database description packets.   | —  |
| <b>OSPF Neighbors</b>    |   |  |
| Address                  | Address of the neighbor.  | —  |
| Interface                | Interface through which the neighbor is reachable.  | —  |
| State                    | State of the neighbor: <b>Attempt, Down, Exchange, ExStart, Full, Init, Loading, or 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 174 on page 1419](#) summarizes key output fields in the BGP routing display in the J-Web user interface.

**Table 174: 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.  | —                      |

Table 174: Summary of Key BGP Routing Output Fields (*continued*)

| Field                | Values  | Additional Information  |
|----------------------|---|---|
| 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.  | —   |
| 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

## Monitoring SCCP ALGs

This section contains the following topics:

- [Monitoring SCCP ALG Calls on page 1421](#)
- [Monitoring SCCP ALG Counters on page 1421](#)

### 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 175 on page 1421](#) summarizes key output fields in the SCCP calls display.

**Table 175: 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 176 on page 1421](#) summarizes key output fields in the SCCP counters display.

**Table 176: 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. | —                      |

Table 176: Summary of Key SCCP Counters Output Fields (*continued*)

| Field                      | Values  | Additional Information |
|----------------------------|---|------------------------|
| 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).                               | —                      |
| 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.                                       | —                      |



Table 176: Summary of Key SCCP Counters Output Fields (*continued*)

| Field              | Values                        | Additional Information |
|--------------------|-------------------------------|------------------------|
| Non specific error | Number of nonspecific errors. | —                      |

- Related Documentation**
- [Monitoring Overview on page 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### [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 177 on page 1423](#) describes the content of this pane.

Table 177: View Policy Log Fields

| Field                | Value   |
|----------------------|---|
| Log file name        | Name of the event log files to search.                        |
| Policy name          | Name of the policy of the events to be retrieved.             |
| Source address       | Source address of the traffic that triggered the event.       |
| Destination address  | Destination address of the traffic that triggered the event.  |
| 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. |

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 178 on page 1424](#) describes the contents of this pane.

**Table 178: 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)

- [Monitoring Alarms on page 1478](#)
- [Monitoring Events on page 1378](#)
- *Junos OS Interfaces Library for Security Devices*

## Monitoring Security Features

This section contains the following topics:

- [Monitoring Policies on page 1425](#)
- [Checking Policies on page 1427](#)
- [Monitoring Screen Counters on page 1430](#)
- [Monitoring IDP Status on page 1432](#)
- [Monitoring Flow Gate Information on page 1433](#)
- [Monitoring Firewall Authentication Table on page 1434](#)
- [Monitoring Firewall Authentication History on page 1436](#)
- [Monitoring 802.1x on page 1438](#)

### 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 179 on page 1425](#) 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 179: 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. |

Table 179: Security Policies Monitoring Output Fields (*continued*)

| Field                 | Value   | Additional Information  |
|-----------------------|---|---|
| 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.  | —   |
| Dynamic App           | Displays the dynamic application signatures to be used as match criteria if an application firewall rule set is configured for the policy.<br><br>For a network firewall, a dynamic application is not defined.   | 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.<br><br>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. |
| Action                | Displays the action portion of the rule set if an application firewall rule set is configured for the policy. <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> | 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.  |

Table 179: Security Policies Monitoring Output Fields (*continued*)

| Field                     | Value  | Additional Information   |
|---------------------------|--|--|
| 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 | 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.  | To toggle a graph on and off, click the counter name below the graph.  |
| 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 180 on page 1428](#) 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 180: 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 180: Check Policies Output (*continued*)

| Field                      | Function  |
|----------------------------|---|
| Protocol                   | Name or equivalent value of the protocol to be matched.<br><br>ah—51<br>egp—8<br>esp—50<br>gre—47<br>icmp—1<br>igmp—2<br>igp—9<br>ipip—94<br>ipv6—41<br>ospf—89<br>pgm—113<br>pim—103<br>rdp—27<br>rsvp—46<br>sctp—132<br>tcp—6<br>udp—17<br>vrrp—112 |
| Result Count               | (Optional) Number of policies to display. Default value is 1. Maximum value is 16.  |
| <b>Check Policies List</b> |   |
| From Zone                  | Name of the source zone.  |
| To Zone                    | Name of the destination zone.   |
| Total Policies             | Number of policies retrieved.   |
| Default Policy action      | The action to be taken if no match occurs.  |
| Name                       | Policy name   |
| Source Address             | Name of the source address (not the IP address) of a policy. Address sets are resolved to their individual names.   |

Table 180: 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 181 on page 1430](#) summarizes key output fields in the screen counters display.

Table 181: 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 181: 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 181: 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 182 on page 1433](#) summarizes key output fields in the IDP display.

Table 182: 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 183 on page 1434](#) summarizes key output fields in the flow gate display.

Table 183: 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 184 on page 1435](#) summarizes key output fields in firewall authentication table display.

Table 184: 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 184: 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 185 on page 1436](#) summarizes key output fields in firewall authentication history display.

Table 185: 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 185: 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 185: 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 186 on page 1438](#) summarizes the Dot1X output fields.

Table 186: 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 186: Summary of Dot1X Output Fields (*continued*)

| Field     | Values                                  | Additional Information |
|-----------|---|------------------------|
| User Name | Name of the authentication-failed user. | —                      |

**Related Documentation**

- [Monitoring Overview on page 1231](#)
- [Monitoring Interfaces on page 1382](#)
- *Junos OS Interfaces Library for Security Devices*

### Monitoring SIP ALGs

This section contains the following topics:

- [Monitoring SIP ALG Calls on page 1439](#)
- [Monitoring SIP ALG Counters on page 1440](#)
- [Monitoring SIP ALG Rate Information on page 1442](#)
- [Monitoring SIP ALG Transactions on page 1442](#)

### 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 187 on page 1439](#) summarizes key output fields in the SIP calls display.

Table 187: 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 188 on page 1440](#) summarizes key output fields in the SIP counters display.

**Table 188: 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. |
| 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.  |

Table 188: Summary of Key SIP Counters Output Fields (*continued*)

| Field                       | Values  | Additional Information   |
|-----------------------------|---|--|
| 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.   | —  |
| 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 189 on page 1442](#) summarizes key output fields in the SIP rate display.

**Table 189: 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. | —                      |
| 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 190 on page 1442](#) summarizes key output fields in the SIP transactions display.

**Table 190: 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> | —                      |

Table 190: Summary of Key SIP Transactions Output Fields (*continued*)

| Field                           | Values  | Additional Information |
|---------------------------------|---|------------------------|
| 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           | <ul style="list-style-type: none"> <li>• <a href="#">Monitoring Overview on page 1231</a></li> <li>• <a href="#">Monitoring Interfaces on page 1382</a></li> <li>• <i>Junos OS Interfaces Library for Security Devices</i></li> </ul>   |                        |
| <b>Monitoring Spanning Tree</b> |   |                        |
| Purpose                         | Use the monitoring functionality to view the Spanning Tree page.  |                        |
| Action                          | To monitor spanning tree, select <b>Monitor&gt;Switching&gt;Spanning Tree</b> in the J-Web user interface.  |                        |
| Meaning                         | <a href="#">Table 191 on page 1443</a> summarizes key output fields in the spanning tree page.  |                        |

Table 191: 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). | —   |

Table 191: Spanning Tree Monitoring Page (*continued*)

| Field                      | Value  | Additional Information |
|----------------------------|--|------------------------|
| Number of topology changes | Total number of STP topology changes detected since the switch last booted.            | –                      |
| Forward delay              | Spanning tree forward delay.   | –                      |
| <b>Interface List</b>      |  |                        |
| Interface Name             | Interface configured to participate in the STP instance.                               | –                      |
| Port ID                    | Logical interface identifier configured to participate in the STP instance.            | –                      |
| Designated Port ID         | Port ID of the designated port for the LAN segment to which the interface is attached. | –                      |
| Port Cost                  | Configured cost for the interface.   | –                      |
| State                      | STP port state. Forwarding (FWD), blocking (BLK), listening, learning, or disabled.    | –                      |
| Role                       | MSTP or RSTP port role. Designated (DESG), backup (BKUP), alternate (ALT), or root.    | –                      |

- Related Documentation**
- [Monitoring Ethernet Switching on page 1377](#)
  - [Monitoring GVRP on page 1380](#)

### 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. On a J Series device, the **Monitor > System View** path provides detailed views of system, chassis, and process information.

This section contains the following topics:

- [Monitoring System Properties for SRX Series Devices on page 1445](#)
- [Monitoring System Properties for J Series Devices on page 1447](#)
- [Monitoring Chassis Information on page 1448](#)
- [Monitoring Process Details for J Series Devices on page 1450](#)
- [System Health Management for Branch SRX Series Devices on page 1451](#)

**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 System Properties for J Series Devices*

**Purpose** View the system properties on a J Series device.

**Action** Select **Monitor>System View>System Information** in the J-Web user interface. The System Information page displays the following types of information:

- **General**—General tab of the System Information page displays the device's serial number, current Junos OS version, hostname, IP address, loopback address, domain name server, and time zone.



**NOTE:** The hostname that appears on this page is defined using the `set system hostname` command.

On J 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.

- **Time**—Time tab of the System Information page displays the current time for the device, the last time the device was booted, the last time protocol settings were configured on the device, and the last time the device configuration was updated. Additionally, this tab displays the CPU load averages for the last 1, 5, and 15 minutes.
- **Storage Media**—Storage Media tab of the System Information page displays information about the memory components installed on the device (such as flash memory or USB) and the amount of memory used compared to total memory available.
- **Logged-In User Details**—Logged-In User Details section of the System Information page displays information about the users who are currently logged into the device, including their usernames, the terminals and systems from which they logged in, the length of their user sessions, and how long their sessions have remained idle.
- **Active User Count**—Active User Count field displays the number of users currently signed into the device.

Alternatively, you can view system properties by entering the following **show** commands in the CLI configuration editor:

- `show system uptime`
- `show system users`
- `show system storage`
- `show version`
- `show chassis hardware`
- `show interface terse`

### ***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 J Series 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`

#### ***Monitoring Process Details for J Series Devices***

**Purpose** View the process details that indicate the status of each of the processes running on the J Series device.

**Action** Select **Monitor>System View>Process Details** in the J-Web user interface.

The Process Details page displays the following types of information for the entire device:

- **CPU Load**—Displays the average CPU usage of the device over the last minute in the form of a graph.
- **Total Memory Utilization**—Displays the current total memory usage of the device in the form of a graph.

The Process Details page also displays the following types of information for each process running on the device:

- **PID**—Displays the unique number identifying the process.
- **Value**—Displays the name of the process.
- **State**—Displays the current state of the process (runnable, sleeping, or unknown).
- **CPU Load**—Displays the current CPU usage of the process.

- Memory Utilization—Displays the current memory usage of the process.
- Start Time—Displays the time that the process started running.

Alternatively, you can view chassis details from the Dashboard on an SRX Series device or by entering the following **show** commands in the CLI configuration editor:

- **show chassis routing-engine**
- **show system process**

### *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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### 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 192 on page 1452](#) summarizes key output fields in the ALG H.323 page.

**Table 192: 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

Table 192: ALG H.323 Monitoring Page (*continued*)

| Field                        | Value  | Additional Information |
|------------------------------|--|------------------------|
| Category                     | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Packets received</b>—Number of ALG 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.  | —                      |
| <b>H.323 Error Counter</b>   |  |                        |
| Category                     | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Decoding errors</b>—Number of decoding errors.</li> <li>• <b>Message flood dropped</b>—Error counter for message flood dropped.</li> <li>• <b>NAT errors</b>—H.323 ALG NAT errors.</li> <li>• <b>Resource manager errors</b>—H.323 ALG resource manager errors.</li> <li>• <b>DSCP Marked errors</b>—H.323 ALG DSCP marked errors.</li> </ul>   | —                      |
| Count                        | Provides count of response codes for each H.323 error counter category.  | —                      |
| <b>Counter Summary Chart</b> |  |                        |
| Packets Received             | Provides the graphical representation of the packets received.   | —                      |
| <b>H.323 Message Counter</b> |  |                        |

Table 192: ALG H.323 Monitoring Page (*continued*)

| Field    | Value   | Additional Information |
|----------|---|------------------------|
| 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 1465](#)
  - [Monitoring Voice ALG MGCP on page 1454](#)
  - [Monitoring Voice ALG SCCP on page 1457](#)
  - [Monitoring Voice ALG SIP on page 1460](#)

### 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 193 on page 1455](#) summarizes key output fields in the voice ALG MGCP page.



Table 193: 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.  | — |

##### MGCP Error Counter

Table 193: Voice ALG MGCP Monitoring Page (*continued*)

| Field                       | Value  | Additional Information |
|-----------------------------|--|------------------------|
| Category                    | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>Unknown-method</b>— MGCP ALG unknown method errors.</li> <li>• <b>Decoding error</b>— MGCP ALG decoding errors.</li> <li>• <b>Transaction error</b>— MGCP ALG transaction errors.</li> <li>• <b>Call error</b>— MGCP ALG call ounter errors.</li> <li>• <b>Connection error</b>— MGCP ALG connection errors.</li> <li>• <b>Connection flood drop</b>— MGCP ALG connection flood drop errors.</li> <li>• <b>Message flood drop</b>— MGCP ALG message flood drop error.</li> <li>• <b>IP resolve error</b>— MGCP ALG IP address resolution errors.</li> <li>• <b>NAT error</b>— MGCP ALG NAT errors.</li> <li>• <b>Resource manager error</b>— MGCP ALG resource manager errors.</li> <li>• <b>DSCP Marked error</b>— MGCP ALG DSCP marked errors.</li> </ul> | —                      |
| Count                       | Provides the count of response codes for each summary error counter category.  | —                      |
| Counter Summary Chart       | Displays the Counter Summary Chart.  | —                      |
| <b>MGCP Packet Counters</b> |  |                        |
| Category                    | Displays the following categories: <ul style="list-style-type: none"> <li>• <b>CRCX</b>— Create Connection</li> <li>• <b>MDCX</b>— Modify Connection</li> <li>• <b>DLCX</b>— Delete Connection</li> <li>• <b>AUEP</b>— Audit Endpoint</li> <li>• <b>AUCX</b>— Audit Connection</li> <li>• <b>NTFY</b>— Notify MGCP</li> <li>• <b>RSIP</b>— Restart in Progress</li> <li>• <b>EPCF</b>— Endpoint Configuration</li> <li>• <b>RQNT</b>— Request for Notification</li> <li>• <b>000-199</b>—Respond code is 0-199</li> <li>• <b>200-299</b>—Respond code is 200-299</li> <li>• <b>300-399</b>—Respond code is 300-399</li> </ul>  | —                      |
| Count                       | Provides count of response codes for each MGCP packet counter category.  | —                      |
| <b>Calls</b>                |  |                        |

Table 193: Voice ALG MGCP Monitoring Page (*continued*)

| Field         | Value  | Additional Information |
|---------------|--|------------------------|
| Endpoint@GW   | Displays the endpoint name.  | —                      |
| Zone          | Displays the following options: <ul style="list-style-type: none"> <li>• <b>trust</b>—Trust zone.</li> <li>• <b>untrust</b>—Untrust zone.</li> </ul> | —                      |
| Endpoint IP   | Displays the endpoint IP address.  | —                      |
| Call ID       | Displays the call identifier for ALG MGCP.   | —                      |
| RM Group      | Displays the resource manager group ID.  | —                      |
| Call Duration | Displays the duration for which connection is active.  | —                      |

- Related Documentation**
- [Monitoring Voice ALG Summary on page 1465](#)
  - [Monitoring Voice ALG H.323 on page 1452](#)
  - [Monitoring Voice ALG SCCP on page 1457](#)
  - [Monitoring Voice ALG SIP on page 1460](#)

### 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 194 on page 1457](#) summarizes key output fields in the voice ALG SCCP page.

Table 194: 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 194: 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 194: 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 1465](#)

- [Monitoring Voice ALG H.323 on page 1452](#)
- [Monitoring Voice ALG MGCP on page 1454](#)
- [Monitoring Voice ALG SIP on page 1460](#)

### 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 195 on page 1460](#) summarizes key output fields in the voice ALG SIP page.

**Table 195: 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 195: Voice ALG SIP Monitoring Page (*continued*)

| Field  | Value | Additional Information |
|--------|-------|------------------------|
| Method |       | —                      |

Table 195: Voice ALG SIP Monitoring Page (*continued*)

| Field | Value  | Additional Information |
|-------|--|------------------------|
|       | <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> <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</li> </ul> |                        |



Table 195: Voice ALG SIP Monitoring Page (*continued*)

| Field                     | Value  | Additional Information |
|---------------------------|--|------------------------|
|                           | <p>server. It is a standard SIP message and will be forwarded until it reaches the server or end user that is performing the service.</p> <ul style="list-style-type: none"> <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.  | —                      |
| Method                    | Displays the call method used.   | —                      |
| State                     | Displays the state of the ALG SIP.   | —                      |
| Group ID                  | Displays the group identifier.   | —                      |
| Invite Method Chart       | <p>Displays the invite method chart. The available options are:</p> <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> | —                      |
| <b>SIP Error Counters</b> |  |                        |

Table 195: 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 1465](#)
  - [Monitoring Voice ALG H.323 on page 1452](#)
  - [Monitoring Voice ALG MGCP on page 1454](#)
  - [Monitoring Voice ALG SCCP on page 1457](#)

### 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 196 on page 1465](#) summarizes key output fields in the voice ALG summary page.

**Table 196: 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 1452](#)
  - [Monitoring Voice ALG MGCP on page 1454](#)
  - [Monitoring Voice ALG SCCP on page 1457](#)
  - [Monitoring Voice ALG SIP on page 1460](#)

## Monitoring VPNs

This section contains the following topics:

- [Monitoring IKE Gateway Information on page 1466](#)
- [Monitoring IPsec VPN—Phase I on page 1469](#)
- [Monitoring IPsec VPN—Phase II on page 1470](#)
- [Monitoring IPsec VPN Information on page 1471](#)

### 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 197 on page 1466](#) summarizes key output fields in the IKE gateway display.

**Table 197: 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.  | —   |

Table 197: Summary of Key IKE SA Information Output Fields (*continued*)

| Field                                      | Values   | Additional Information   |
|--|--|--|
| 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                                       | <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 197: 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 197: 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 198 on page 1469](#) describes the available options for monitoring IPsec VPN-Phase I.

Table 198: 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 198: 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 199 on page 1470](#) describes the available options for monitoring IPsec VPN-Phase II.

Table 199: IPsec VPN—Phase II Monitoring Page

| Field                  | Values | Additional Information |
|------------------------|--------|------------------------|
| Statistics Tab Details |        |                        |



Table 199: 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 200 on page 1472 summarizes key output fields in the IPsec VPN display.

**Table 200: 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 200: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field                        | Values  | Additional Information |
|------------------------------|---|------------------------|
| Vsys                         | The root system.  | —                      |
| IPsec Statistics Information |   |                        |
| ESP Statistics               | <p>Encapsulation Security Protocol (ESP) statistics include the following:</p> <ul style="list-style-type: none"> <li>• <b>Encrypted bytes</b>—Total number of bytes encrypted by the local system across the IPsec tunnel.</li> <li>• <b>Decrypted bytes</b>—Total number of bytes decrypted by the local system across the IPsec tunnel.</li> <li>• <b>Encrypted packets</b>—Total number of packets encrypted by the local system across the IPsec tunnel.</li> <li>• <b>Decrypted packets</b>—Total number of packets decrypted by the local system across the IPsec tunnel.</li> </ul>   | —                      |
| AH Statistics                | <p>Authentication Header (AH) statistics include the following:</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—The number of bytes presented for processing by the device.</li> <li>• <b>Output bytes</b>—The number of bytes actually processed by the device.</li> <li>• <b>Input packets</b>—The number of packets presented for processing by the device.</li> <li>• <b>Output packets</b>—The number of packets actually processed by the device.</li> </ul>  | —                      |
| Errors                       | <p>Errors include the following</p> <ul style="list-style-type: none"> <li>• <b>AH authentication failures</b>—Total number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel.</li> <li>• <b>Replay errors</b>—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window.</li> <li>• <b>ESP authentication failures</b>—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets.</li> <li>• <b>ESP decryption failures</b>—Total number of ESP decryption errors.</li> <li>• <b>Bad headers</b>—Total number of invalid headers detected.</li> <li>• <b>Bad trailers</b>—Total number of invalid trailers detected.</li> </ul> | —                      |

Table 200: Summary of Key IPsec VPN Information Output Fields (*continued*)

| Field  | Values  | Additional Information |
|--|---|------------------------|
| <b>Details for IPsec SA Index: <i>ID</i></b> |   |                        |
| 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 200: 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 200: 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### 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 1231](#)
  - [Monitoring Interfaces on page 1382](#)
  - *Junos OS Interfaces Library for Security Devices*

### 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 # #

- You can click the **Clear Web Filtering Statistics** button to clear all current viewable statistics and begin collecting new statistics.

#### Related Documentation

- [UTM Web Filtering Feature Guide for Security Devices](#)
- [Web Filtering Overview](#)
- [Understanding Integrated Web Filtering](#)
- [Example: Configuring Local Web Filtering](#)

## Alarms

- [Monitoring Active Alarms on a Device on page 1477](#)
- [Monitoring Alarms on page 1478](#)

### 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 1237](#)
- [Example: Configuring Interface Alarms on page 1276](#)
- [Monitoring Alarms on page 1478](#)

### 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 201 on page 1478](#) summarizes key output fields in the alarms page.

**Table 201: Alarms Monitoring Page**

| Field               | Value   | Additional Information |
|---------------------|---|------------------------|
| <b>Alarm Filter</b> |   |                        |
| Alarm Type          | Specifies the type of alarm to monitor: <ul style="list-style-type: none"> <li>• <b>System</b>— System alarms include FRU detection alarms (power supplies removed, for instance).</li> <li>• <b>Chassis</b>— Chassis alarms indicate environmental alarms such as temperature.</li> <li>• <b>All</b>— Indicates to display all the types of alarms.</li> </ul> | —                      |



Table 201: Alarms Monitoring Page (*continued*)

| Field         | Value   | Additional Information |
|---------------|---|------------------------|
| Severity      | Specifies the alarm severity that you want to monitor <ul style="list-style-type: none"> <li>• <b>Major</b>— A major (red) alarm condition requires immediate action.</li> <li>• <b>Minor</b>— A minor (yellow) condition requires monitoring and maintenance.</li> <li>• <b>All</b>— Indicates to display all the severities.</li> </ul>                   | —                      |
| 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"> <li>• <b>Type</b>— Type of alarm: System, Chassis, or All.</li> <li>• <b>Severity</b>— Severity class of the alarm: Minor or Major.</li> <li>• <b>Description</b>— Description of the alarm.</li> <li>• <b>Time</b>— Time that the alarm was registered.</li> </ul> | —                      |

- Related Documentation**
- [Monitoring Active Alarms on a Device on page 1477](#)
  - [Monitoring Events on page 1378](#)
  - [Monitoring Security Events by Policy on page 1423](#)

## Data Path Debugging and Trace Options

- [Displaying a List of Devices on page 1480](#)
- [Displaying Log and Trace Files on page 1481](#)
- [Displaying Output for Security Trace Options on page 1481](#)
- [Displaying Multicast Trace Operations on page 1482](#)

- [Using the J-Web Traceroute Tool on page 1483](#)
- [J-Web Traceroute Results and Output Summary on page 1484](#)

### 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 202 on page 1480](#) describes the **traceroute** command options.

**Table 202: CLI traceroute Command Options**

| Option  | Description  |
|---|--|
| <i>host</i>                                   | Sends traceroute packets to the hostname or IP address you specify.  |
| <i>interface interface-name</i>               | (Optional) Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.  |
| <i>as-number-lookup</i>                       | (Optional) Displays the autonomous system (AS) number of each intermediate hop between the device and the destination host.  |
| <i>bypass-routing</i>                         | (Optional) Bypasses the routing tables and sends the traceroute packets only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.<br><br>Use this option to display a route to a local system through an interface that has no route through it. |
| <i>gateway address</i>                        | (Optional) Uses the gateway you specify to route through.  |
| <i>inet</i>                                   | (Optional) Forces the traceroute packets to an IPv4 destination.   |
| <i>inet6</i>                                  | (Optional) Forces the traceroute packets to an IPv6 destination.   |
| <i>no-resolve</i>                             | (Optional) Suppresses the display of the hostnames of the hops along the path.   |
| <i>routing-instance routing-instance-name</i> | (Optional) Uses the routing instance you specify for the traceroute.   |
| <i>source address</i>                         | (Optional) Uses the source address that you specify, in the traceroute packet.   |
| <i>tos number</i>                             | (Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255.   |
| <i>tll number</i>                             | (Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 128.  |
| <i>wait seconds</i>                           | (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.

### 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.

### 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 1243](#)
  - [Setting Security Trace Options \(CLI Procedure\) on page 1279](#)

## 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 203 on page 1482](#) summarizes the output fields of the display.

**Table 203: CLI mtrace monitor Command Output Summary**

| Field                                       | Description   |
|---|---|
| <b>Mtrace operation-type at time-of-day</b> | <ul style="list-style-type: none"> <li>• <b>operation-type</b>—Type of multicast trace operation: <b>query</b> or <b>response</b>.</li> <li>• <b>time-of-day</b>—Date and time the multicast trace query or response was captured.</li> </ul> |
| <b>by</b>                                   | IP address of the host issuing the query.   |
| <b>resp to address</b>                      | <b>address</b> —Response destination address.   |
| <b>qid qid</b>                              | <b>qid</b> —Query ID number.  |
| <b>packet from source to destination</b>    | <ul style="list-style-type: none"> <li>• <b>source</b>—IP address of the source of the query or response.</li> <li>• <b>destination</b>—IP address of the destination of the query or response.</li> </ul>                                    |
| <b>from source to destination</b>           | <ul style="list-style-type: none"> <li>• <b>source</b>—IP address of the multicast source.</li> <li>• <b>destination</b>—IP address of the multicast destination.</li> </ul>  |
| <b>via group address</b>                    | <b>address</b> —Group address being traced.   |
| <b>mxhop=number</b>                         | <b>number</b> —Maximum hop setting.   |

- Related Documentation**
- [Using the J-Web Traceroute Tool on page 1483](#)
  - [J-Web Traceroute Results and Output Summary on page 1484](#)

### 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 204 on page 1483](#)).

**Table 204: Traceroute Field Summary**

| Field                   | Function  | Your Action  |
|-------------------------|---|--|
| Remote Host             | Identifies the destination host of the traceroute.<br><br>The <b>Remote Host</b> field is the only required field.  | Type the hostname or IP address of the destination host.   |
| <b>Advanced Options</b> |   |  |
| Don't Resolve Addresses | Determines whether hostnames of the hops along the path are displayed, in addition to IP addresses.   | <ul style="list-style-type: none"> <li>• Suppress the display of the hop hostnames by selecting the check box.</li> <li>• Display the hop hostnames by clearing the check box.</li> </ul>  |
| Gateway                 | Specifies the IP address of the gateway to route through.   | Type the gateway IP address.   |
| Source Address          | Specifies the source address of the outgoing traceroute packets.  | Type the source IP address.  |
| Bypass Routing          | <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> |

Table 204: Traceroute Field Summary (*continued*)

| Field              | Function  | Your Action   |
|--------------------|---|---|
| Interface          | Specifies the interface on which the traceroute packets are sent.   | Select the interface on which traceroute packets are sent from the list. If you select <b>any</b> , the traceroute requests are sent on all interfaces.                         |
| Time-to-Live       | Specifies the maximum time-to-live (TTL) hop count for the traceroute request packet.   | Select the TTL from the list.   |
| Type-of-Service    | Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.                                 | Select the decimal value of the TOS field from the list.  |
| Resolve AS Numbers | Determines whether the autonomous system (AS) number of each intermediate hop between the device and the destination host is displayed. | <ul style="list-style-type: none"> <li>Display the AS numbers by selecting the check box.</li> <li>Suppress the display of the AS numbers by clearing the check box.</li> </ul> |

4. Click **Start**.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

*hop-number host (ip-address) [as-number]time1 time2 time3*

The device sends a total of three traceroute packets to each router along the path and the round-trip time for each traceroute operation appears. If the device times out before receiving a **Time Exceeded** message, an asterisk (\*) appears for that round-trip time.

5. You can stop the traceroute operation before it is complete by clicking **OK** while the results of the traceroute operation appear.

#### Related Documentation

- [Diagnostic Tools Overview on page 1232](#)
- [J-Web Traceroute Results and Output Summary on page 1484](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)
- *Junos OS Interfaces Library for Security Devices*

#### J-Web Traceroute Results and Output Summary

Table 205 on page 1484 summarizes the output in the traceroute display.

Table 205: J-Web Traceroute Results and Output Summary

| Field             | Description                                |
|-------------------|--|
| <i>hop-number</i> | Number of the hop (device) along the path. |

Table 205: J-Web Traceroute Results and Output Summary (*continued*)

| Field             | Description  |
|-------------------|--|
| <i>host</i>       | Hostname, if available, or IP address of the device. If the Don't Resolve Addresses check box is selected, the hostname does not appear.                     |
| <i>ip-address</i> | IP address of the device.  |
| <i>as-number</i>  | AS number of the device.   |
| <i>time1</i>      | Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.  |
| <i>time2</i>      | Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device. |
| <i>time3</i>      | Round-trip time between the sending of the third traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular device.  |

If the device does not display the complete path to the destination host, one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host, or a router along the path, might be configured to ignore ICMP traceroute messages.
- The host, or a device along the path, might be configured with a firewall filter that blocks ICMP traceroute requests or ICMP time exceeded responses.
- The value you selected in the Time Exceeded box was less than the number of hops in the path to the host. In this case, the host might reply with an ICMP error message.

#### Related Documentation

- [Diagnostic Tools Overview on page 1232](#)
- [Using the J-Web Traceroute Tool on page 1483](#)
- [Junos OS Interfaces Library for Security Devices](#)

## MPLS

- [Using the ping Command on page 1486](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [J-Web Ping Host Results and Output Summary on page 1490](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- [J-Web Ping MPLS Results and Output Summary on page 1494](#)
- [Pinging Layer 2 Circuits on page 1494](#)
- [Pinging Layer 2 VPNs on page 1495](#)

- [Pinging Layer 3 VPNs on page 1497](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1498](#)

### 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 206 on page 1486](#) describes the **ping** command options.

To quit the **ping** command, press Ctrl-C.

**Table 206: CLI ping Command Options**

| Option                            | Description   |
|-----------------------------------|---|
| <i>host</i>                       | Pings the hostname or IP address you specify.   |
| <i>interface source-interface</i> | (Optional) Sends the ping requests on the interface you specify. If you do not include this option, ping requests are sent on all interfaces.   |
| <i>bypass-routing</i>             | (Optional) Bypasses the routing tables and sends the ping requests only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.<br><br>Use this option to ping a local system through an interface that has no route through it. |
| <i>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.  |



Table 206: CLI ping Command Options (*continued*)

| Option   | Description   |
|--|---|
| <b>pattern <i>string</i></b>                         | (Optional) Includes the hexadecimal string you specify, in the ping request packet.   |
| <b>rapid</b>   | (Optional) Sends ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the <b>count</b> option.   |
| <b>record-route</b>                                  | (Optional) For IPv4, sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed on the screen.   |
| <b>routing-instance <i>routing-instance-name</i></b> | (Optional) Uses the routing instance you specify for the ping request.  |
| <b>size <i>bytes</i></b>                             | (Optional) Sets the size of the ping request packet. Specify a size from <b>0</b> through <b>65,468</b> . The default value is <b>56</b> bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.  |
| <b>source <i>source-address</i></b>                  | (Optional) Uses the source address that you specify, in the ping request packet.  |
| <b>strict</b>  | (Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.   |
| <b>strict-source [<i>hosts</i>]</b>                  | (Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet, and uses the list of hosts you specify for routing the packet.  |
| <b>tos <i>number</i></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 <i>number</i></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 <i>seconds</i></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 J Series 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 1232](#)
  - [Configuring Ping MPLS on page 1281](#)
  - [Pinging Layer 2 Circuits on page 1494](#)
  - [Pinging Layer 2 VPNs on page 1495](#)
  - [Pinging Layer 3 VPNs on page 1497](#)
  - [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1498](#)
  - *Junos OS Interfaces Library 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 J Series 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 1486](#).)

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 207 on page 1488](#)).

**Table 207: J-Web Ping Host Field Summary**

| Field                   | Function   | Your Action   |
|-------------------------|--|---|
| Remote Host             | Identifies the host to ping.<br><br>This is the only required field.               | Type the hostname or IP address of the host to ping.  |
| <b>Advanced Options</b> |  |   |
| Don't Resolve Addresses | Determines whether to display hostnames of the hops along the path.                | <ul style="list-style-type: none"> <li>• Suppress the display of the hop hostnames by selecting the check box.</li> <li>• Display the hop hostnames by clearing the check box.</li> </ul> |
| Interface               | Specifies the interface on which the ping requests are sent.                       | Select the interface on which ping requests are sent from the list. If you select <b>any</b> , the ping requests are sent on all interfaces.  |
| Count                   | Specifies the number of ping requests to send.                                     | Select the number of ping requests to send from the list.   |
| Don't Fragment          | Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet. | <ul style="list-style-type: none"> <li>• Set the DF bit by selecting the check box.</li> <li>• Clear the DF bit by clearing the check box.</li> </ul>                                     |

Table 207: J-Web Ping Host Field Summary (*continued*)

| Field            | Function  | Your Action  |
|------------------|---|--|
| Record Route     | Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.   | <ul style="list-style-type: none"> <li>Record and display the path of the packet by selecting the check box.</li> <li>Suppress the recording and display of the path of the packet by clearing the check box.</li> </ul>                                       |
| Type-of-Service  | Specifies the type-of-service (TOS) value in the IP header of the ping request packet.  | Select the decimal value of the TOS field from the list.   |
| Routing Instance | Names the routing instance for the ping attempt.  | Select the routing instance name from the list.  |
| Interval         | Specifies the interval, in seconds, between the transmission of each ping request.  | Select the interval from the list.   |
| Packet Size      | Specifies the size of the ping request packet.  | Type the size, in bytes, of the packet. The size can be from 0 through 65,468. The device adds 8 bytes of ICMP header to the size.   |
| Source Address   | Specifies the source address of the ping request packet.  | Type the source IP address.  |
| Time-to-Live     | Specifies the time-to-live (TTL) hop count for the ping request packet.   | Select the TTL from the list.  |
| Bypass Routing   | <p>Determines whether ping requests are routed by means of the routing table.</p> <p>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.</p> | <ul style="list-style-type: none"> <li>Bypass the routing table and send the ping requests to hosts on the specified interface only by selecting the check box.</li> <li>Route the ping requests using the routing table by clearing the check box.</li> </ul> |

4. Click **Start**.

The results of the ping operation appear in the main pane. If no options are specified, each ping response is in the following format:

*bytes bytes from ip-address: icmp\_seq=number ttl=number time=time*

5. You can stop the ping operation before it is complete by clicking **OK**.
**Related  
Documentation**

- [Diagnostic Tools Overview on page 1232](#)
- [Configuring Ping MPLS on page 1281](#)
- [J-Web Ping Host Results and Output Summary on page 1490](#)
- [Using the J-Web Traceroute Tool on page 1483](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)

## J-Web Ping Host Results and Output Summary

Table 208 on page 1490 summarizes the output in the ping host display.

**Table 208: Ping Host Results and Output**

| Ping Host Result   | Description   |
|--|---|
| <i>bytes bytes from ip-address</i>   | <ul style="list-style-type: none"> <li><b>bytes</b>—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8.</li> <li><b>ip-address</b>—IP address of destination host that sent the ping response packet.</li> </ul>  |
| <i>icmp_seq=0</i><br><i>icmp_seq=number</i>  | <b>number</b> —Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.  |
| <i>ttl=number</i>  | <b>number</b> —Time-to-live hop-count value of the ping response packet.  |
| <i>number packets transmitted</i>  | <b>number</b> —Number of ping requests (probes) sent to host.   |
| <i>percentage packet loss</i>  | <b>percentage</b> —Number of ping responses divided by the number of ping requests, specified as a percentage.  |
| <i>round-trip min/avg/max/stddev =</i><br><i>min-time/avg-time/max-time/std-dev ms</i> | <ul style="list-style-type: none"> <li><b>min-time</b>—Minimum round-trip time (see <b>time=time</b> field in this table).</li> <li><b>avg-time</b>—Average round-trip time.</li> <li><b>max-time</b>—Maximum round-trip time.</li> <li><b>std-dev</b>—Standard deviation of the round-trip times.</li> </ul> |

If the device does not receive ping responses from the destination host (the output shows a packet loss of 100 percent), one of the following explanations might apply:

- The host is not operational.
- There are network connectivity problems between the device and the host.
- The host might be configured to ignore ICMP echo requests.
- The host might be configured with a firewall filter that blocks ICMP echo requests or ICMP echo responses.
- The size of the ICMP echo request packet exceeds the MTU of a host along the path.
- The value you selected in the Time-to-Live box was less than the number of hops in the path to the host, in which case the host might reply with an ICMP error message.

### Related Documentation

- [Diagnostic Tools Overview on page 1232](#)
- [Configuring Ping MPLS on page 1281](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [Junos OS Interfaces Library 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 J Series 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 209 on page 1491](#)).

**Table 209: 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 J Series 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 J Series 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.                                      |

Table 209: J-Web Ping MPLS Field Summary (*continued*)

| Field  | Function  | Your Action  |
|--|---|--|
| 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 J Series device interface.  |
| <b>Locate LSP using interface name</b>           |   |  |
| Interface  | Specifies the interface on which the ping requests are sent.            | Select the J Series 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 J Series device interface.  |
| Count  | Specifies the number of ping requests to send.                          | Select the number of ping requests to send from the list. The default is 5 requests.   |
| Detailed Output                                  | Requests the display of extensive rather than brief ping output.        | Select the check box to display detailed output.   |
| <b>Instance to which this connection belongs</b> |   |  |
| Layer 2VPN Name                                  | Identifies the Layer 2 VPN to ping.                                     | Type the name of the VPN to ping.  |
| Remote Site Identifier                           | Specifies the remote site identifier of the Layer 2 VPN to ping.        | Type the remote site identifier for the VPN.   |
| Source Address                                   | Specifies the source address of the ping request packet.                | Type the source IP address—a valid address configured on a J Series 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 J Series 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 J Series 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.   |

Table 209: J-Web Ping MPLS Field Summary (*continued*)

| Field  | Function   | Your Action   |
|--|--|---|
| Detailed Output                                    | Requests the display of extensive rather than brief ping output.               | Select the check box to display detailed output.  |
| <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 J Series device interface.           |
| Count  | Specifies the number of ping requests to send.                                 | Select the number of ping requests to send from the list.                                       |
| Detailed Output                                    | Requests the display of extensive rather than brief ping output.               | Select the check box to display detailed output.  |
| <b>Ping end point of LSP</b>                       |  |   |
| VPN Prefix   | Identifies the LSP endpoint to ping.   | Type either the LDP FEC prefix and length or the RSVP LSP endpoint address for the LSP to ping. |
| Source Address                                     | Specifies the source address of the ping request packet.                       | Type the source IP address—a valid address configured on a J Series 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 1232](#)
- [Configuring Ping MPLS on page 1281](#)
- [J-Web Ping MPLS Results and Output Summary on page 1494](#)
- [Using the J-Web Traceroute Tool on page 1483](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)

## J-Web Ping MPLS Results and Output Summary

Table 210 on page 1494 summarizes the output in the ping MPLS display.

**Table 210: J-Web Ping MPLS Results and Output Summary**

| Field                             | Description   |
|-----------------------------------|---|
| Exclamation point (!)             | Echo reply was received.  |
| Period (.)                        | Echo reply was not received within the timeout period.  |
| x                                 | Echo reply was received with an error code. Errored packets are not counted in the received packets count and are accounted for separately.   |
| <i>number</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 1232](#)
- [Configuring Ping MPLS on page 1281](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- *Junos OS Interfaces Library 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 211 on page 1495 describes the **ping mpls l2circuit** command options.

**Table 211: 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</b> <b>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 1486](#)
- [Configuring Ping MPLS on page 1281](#)
- [Pinging Layer 2 VPNs on page 1495](#)
- [Pinging Layer 3 VPNs on page 1497](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1498](#)
- [Using the J-Web Ping Host Tool on page 1488](#)

#### 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 212 on page 1496 describes the **ping mpls l2vpn** command options.

Table 212: 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

--- 1ping 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 1486](#)
- [Configuring Ping MPLS on page 1281](#)
- [Pinging Layer 2 Circuits on page 1494](#)
- [Pinging Layer 3 VPNs on page 1497](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1498](#)
- [Using the J-Web Ping Host Tool on page 1488](#)

**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 213 on page 1497](#) describes the **ping mpls l3vpn** command options.

**Table 213: 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 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 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
!!!!!
--- 1ping 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 1486](#)
- [Configuring Ping MPLS on page 1281](#)
- [Pinging Layer 2 Circuits on page 1494](#)
- [Pinging Layer 2 VPNs on page 1495](#)
- [Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 1498](#)
- [Using the J-Web Ping Host Tool on page 1488](#)

**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 214 on page 1498](#) describes the **ping mpls** command options.

**Table 214: 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
--- 1sping 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 1486](#)
  - [Configuring Ping MPLS on page 1281](#)
  - [Pinging Layer 2 Circuits on page 1494](#)
  - [Pinging Layer 2 VPNs on page 1495](#)
  - [Pinging Layer 3 VPNs on page 1497](#)
  - [Using the J-Web Ping Host Tool on page 1488](#)

## Packet Capture

- [Displaying Packet Headers on page 1499](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)
- [J-Web Packet Capture Results and Output Summary on page 1506](#)

### 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 215 on page 1499 describes the **monitor traffic** command options.

**Table 215: CLI monitor traffic Command Options**

Option	Description
<b>absolute-sequence</b>	(Optional) Displays the absolute TCP sequence numbers.
<b>count number</b>	(Optional) Displays the specified number of packet headers. Specify a value from 0 through 100,000. The command quits and exits to the command prompt after this number is reached.
<b>interface interface-name</b>	(Optional) Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.
<b>layer2-headers</b>	(Optional) Displays the link-layer packet header on each line.

Table 215: 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 216 on page 1501</a> through <a href="#">Table 218 on page 1503</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 216 on page 1501](#), enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in [Table 217 on page 1502](#) (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 218 on page 1503](#) (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in [Table 218 on page 1503](#).
- Binary—Expressions that use the binary operators listed in [Table 218 on page 1503](#).
- Packet data accessor—Expressions that use the following syntax:

```
protocol [byte-offset <size>]
```

Replace *protocol* with any protocol in [Table 216 on page 1501](#). 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 216: 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 216: 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 217: 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 218: 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 1246](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)
- [Changing Encapsulation on Interfaces with Packet Capture Configured on page 1293](#)
- [Example: Configuring Packet Capture on an Interface on page 1286](#)

#### 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 219 on page 1504](#)). 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 219: 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 219: 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 219: 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 1246](#)
- [Diagnostic Tools Overview on page 1232](#)
- [J-Web Packet Capture Results and Output Summary on page 1506](#)
- [Using the J-Web Ping MPLS Tool on page 1491](#)
- [Using the J-Web Ping Host Tool on page 1488](#)
- [Using the J-Web Traceroute Tool on page 1483](#)
- *Junos OS Interfaces Library for Security Devices*

### [J-Web Packet Capture Results and Output Summary](#)

[Table 220 on page 1507](#) summarizes the output in the packet capture display.

Table 220: 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 1246](#)
- [Diagnostic Tools Overview on page 1232](#)
- [Using the J-Web Packet Capture Tool on page 1503](#)
- *Junos OS Interfaces Library for Security Devices*

## RPM

- [Monitoring RPM Probes on page 1507](#)

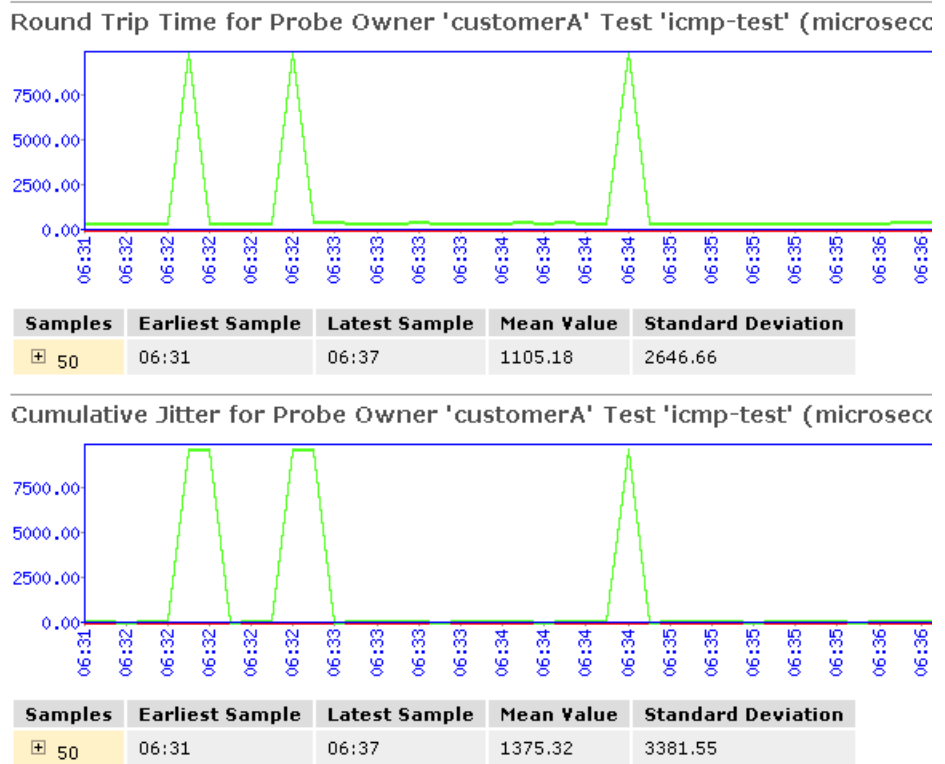
### Monitoring RPM Probes

The RPM information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the device. To view these RPM properties, select **Troubleshoot>RPM>View RPM** in the J-Web user interface, or in configuration mode enter the **show** command:

```
[edit]
user@host# run show services rpm probe-results
```

In addition to the RPM statistics for each RPM test, the J-Web user interface displays the round-trip times and cumulative jitter graphically. [Figure 40 on page 633](#) shows sample graphs for an RPM test.

**Figure 55: Sample RPM Graphs**



In [Figure 40 on page 633](#), 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 221 on page 1508](#) summarizes key output fields in RPM displays.

**Table 221: 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.	—
Test Name	Configured name of the RPM test.	—

Table 221: Summary of Key RPM Output Fields (*continued*)

Field	Values	Additional Information
Probe Type	Type of RPM probe configured for the specified test: <ul style="list-style-type: none"> <li>• <b>http-get</b></li> <li>• <b>http-get-metadata</b></li> <li>• <b>icmp-ping</b></li> <li>• <b>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.	–
Latest Sample	System time when the last probe in the sample was received.	–

Table 221: Summary of Key RPM Output Fields (*continued*)

Field	Values	Additional Information
Mean Value	Average round-trip time for the 50-probe sample.	–
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	–
Lowest Value	Shortest round-trip time from the device to the remote server, as measured over the 50-probe sample.	–
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	–
Highest Value	Longest round-trip time from the Juniper Networks device to the remote server, as measured over the 50-probe sample.	–
Time of Highest Sample	System time when the highest value in the 50-probe sample was received.	–
<b>Cumulative Jitter for a Probe</b>		
Samples	Total number of probes used for the data set.	The Juniper Networks device maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	–
Latest Sample	System time when the last probe in the sample was received.	–
Mean Value	Average jitter for the 50-probe sample.	–
Standard Deviation	Standard deviation of the jitter values for the 50-probe sample.	–
Lowest Value	Smallest jitter value, as measured over the 50-probe sample.	–
Time of Lowest Sample	System time when the lowest value in the 50-probe sample was received.	–
Highest Value	Highest jitter value, as measured over the 50-probe sample.	–
Time of Highest Sample	System time when the highest jitter value in the 50-probe sample was received.	–



- Related Documentation**
- [RPM Overview on page 1248](#)
  - [RPM Support for VPN Routing and Forwarding on page 1252](#)
  - [RPM Configuration Options on page 1306](#)

## Operational Commands

- [monitor list](#)
- [monitor start](#)
- [monitor stop](#)
- [monitor traffic](#)
- [mtrace monitor](#)
- [ping mpls l2vpn](#)
- [ping mpls l2circuit](#)
- [ping mpls l3vpn](#)
- [ping mpls ldp](#)
- [ping mpls lsp-end-point](#)
- [ping mpls rsvp](#)
- [request pppoe connect](#)
- [request pppoe disconnect](#)
- [show configuration](#)
- [show chassis alarms](#)
- [show interfaces \(SRX Series\)](#)
- [show poe interface \(View\)](#)
- [show poe telemetries interface \(View\)](#)
- [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 rpm probe-results \(View\)](#)
- [show system alarms](#)
- [traceroute](#)

## 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 1513</a></li> <li><a href="#">monitor stop on page 1515</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor list on page 1512</a>
<b>Output Fields</b>	<a href="#">Table 222 on page 1512</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 222: 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 1512</a></li> <li>• <a href="#">monitor stop on page 1515</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor start on page 1514</a>
<b>Output Fields</b>	<a href="#">Table 223 on page 1513</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 223: 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 1512</a></li> <li>• <a href="#">monitor start on page 1513</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor stop on page 1515</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`.

`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 224 on page 1518](#).

Table 224: 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 224: 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 225 on page 1519](#).

Table 225: 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 225: 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 226 on page 1521](#).



**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 224 on page 1518](#).
- 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 226: 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 1522](#)  
[monitor traffic detail count on page 1522](#)  
[monitor traffic extensive \(Absolute Sequence\) on page 1522](#)  
[monitor traffic extensive \(Relative Sequence\) on page 1522](#)  
[monitor traffic extensive count on page 1522](#)  
[monitor traffic interface on page 1523](#)  
[monitor traffic matching on page 1523](#)  
[monitor traffic \(TX Matrix Plus Router\) on page 1523](#)  
[monitor traffic \(QFX3500 Switch\) on page 1524](#)

**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.com4.65235 >

```

```

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.com4.65235: P 1:241(240) ack 0 win 33304

<nop,nop,timestamp 993590 42366734>
04:12:00.022900
In IP f4.65235 >
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 1527</a>
<b>Output Fields</b>	<a href="#">Table 227 on page 1526</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 227: 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 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 <i>count</i></b>—(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 <i>address</i></b>—(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 <i>forwarding-class</i></b>—(Optional) Value of the forwarding class for the MPLS ping packets.</p> <p><b>instance <i>instance-name</i> local-site-id <i>local-site-id-number</i> remote-site-id <i>remote-site-id-number</i></b>—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 <i>interface-name</i></b>—Ping an interface configured for the Layer 2 VPN on the egress PE router or switch.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(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 1529</a>  <a href="#">ping mpls l2vpn instance detail on page 1530</a>  <a href="#">ping mpls l2vpn interface &lt;interface-name&gt; reply-mode on page 1530</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 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.  
 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 1532](#)  
[ping mpls l2circuit virtual-circuit detail on page 1532](#)  
[ping mpls l2circuit interface <interface-name> reply-mode on page 1533](#)

**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 l3vpn

<b>Syntax</b>	<pre>ping mpls l3vpn prefix <i>prefix-name</i> &lt;<i>l3vpn-name</i>&gt; &lt;bottom-label-ttl&gt; &lt;count <i>count</i>&gt; &lt;destination <i>address</i>&gt; &lt;detail&gt; &lt;exp <i>forwarding-class</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>
<b>Description</b>	<p>Check the operability of a MPLS Layer 3 virtual private network (VPN) connection. Type Ctrl+c to interrupt a <b>ping mpls l3vpn</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 <i>count</i></b>—(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 <i>address</i></b>—(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 <i>forwarding-class</i></b>—(Optional) Value of the forwarding class for the MPLS ping packets.</p> <p><b><i>l3vpn-name</i></b>—(Optional) Layer 3 VPN name.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on the specified logical system.</p> <p><b>prefix <i>prefix-name</i></b>—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.</p> <p><b>size <i>bytes</i></b>—(Optional) Size of the label-switched path (LSP) ping request packet (<b>96</b> through <b>65468</b> 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.</p>



**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.

**Required Privilege Level** network

**List of Sample Output** [ping mpls l3vpn on page 1535](#)  
[ping mpls l3vpn detail on page 1535](#)

**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
!!!!
--- lsping 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
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

## ping mpls ldp

<b>Syntax</b>	<pre>ping mpls ldp fec &lt;count count&gt; &lt;destination address&gt; &lt;detail&gt; &lt;exp forwarding-class&gt; &lt;instance routing-instance-name&gt; &lt;logical-system (all   logical-system-name)&gt; &lt;p2mp root-addr ip-address lsp-id identifier&gt; &lt;size bytes&gt; &lt;source source-address&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>
<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 forwarding-class</b>—(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> (<b>all</b>   <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 than the minimum size, an error message is displayed reminding you of the 88-byte minimum.</p>

**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. .

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 1537](#)  
[ping mpls ldp p2mp root-addr lsp-id on page 1537](#)

**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--- 1sping 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>
<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 <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>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 <b>88</b> bytes. If the endpoint is RSVP-based, the minimum size of the packet is <b>100</b> bytes. The maximum size in either case is <b>65468</b> 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 (<b>lo.0</b>).</p> <p><b>sweep</b>—(Optional) Automatically determine the size of the maximum transmission unit (MTU).</p>

**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 1540](#)

**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 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.

**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 1543](#)  
[ping mpls rsvp \(Echo Reply with Error Code\) on page 1543](#)



[ping mpls rsvp detail on page 1543](#)

[ping mpls rsvp multipoint egress detail count on page 1543](#)

[ping mpls rsvp multipoint detail count on page 1543](#)

[ping mpls rsvp destination detail count size on page 1544](#)

[ping mpls rsvp destination detail sweep size on page 1544](#)

**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 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 1546</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 1547</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
```

## show configuration

---

**Syntax**    `show configuration`  
              `<statement-path>`

**Release Information**    Command introduced before Junos OS Release 7.4.  
                              Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**    Display the configuration that currently is running on the router or switch, which is the last committed configuration.

**Options**    **none**—Display the entire configuration.

**statement-path**—(Optional) Display one of the following hierarchies in a configuration. (Each **statement-path** option has additional suboptions not described here. See the appropriate feature guide or EX Series switch documentation for more information.)

- **access**—Network access configuration.
- **access-profile**—Access profile configuration.
- **accounting-options**—Accounting data configuration.
- **applications**—Applications defined by protocol characteristics.
- **apply-groups**—Groups from which configuration data is inherited.
- **chassis**—Chassis configuration.
- **chassis network-services**—Current running mode.
- **class-of-service**—Class-of-service configuration.
- **diameter**—Diameter base protocol layer configuration.
- **ethernet-switching-options**—(EX Series switch only) Ethernet switching configuration.
- **event-options**—Event processing configuration.
- **firewall**—Firewall configuration.
- **forwarding-options**—Options that control packet sampling.
- **groups**—Configuration groups.
- **interfaces**—Interface configuration.
- **jsrc**—JSRC partition configuration.
- **jsrc-partition**—JSRC partition configuration.
- **logical-systems**—Logical system configuration.
- **poe**—(EX Series switch only) Power over Ethernet configuration.
- **policy-options**—Routing policy option configuration.
- **protocols**—Routing protocol configuration.

- **routing-instances**—Routing instance configuration.
- **routing-options**—Protocol-independent routing option configuration.
- **security**—Security configuration.
- **services**—Service PIC applications configuration.
- **snmp**—Simple Network Management Protocol configuration.
- **system**—System parameters configuration.
- **virtual-chassis**—(EX Series switch only) Virtual Chassis configuration.
- **vlan**—(EX Series switch only) VLAN configuration.

**Additional Information** The portions of the configuration that you can view depend on the user class that you belong to and the corresponding permissions. If you do not have permission to view a portion of the configuration, the text **ACCESS-DENIED** is substituted for that portion of the configuration. If you do not have permission to view authentication keys and passwords in the configuration, because the **secret** permission bit is not set for your user account, the text **SECRET-DATA** is substituted for that portion of the configuration. If an identifier in the configuration contains a space, the identifier is displayed in quotation marks.

**Required Privilege Level** view

**Related Documentation**

- [Displaying the Current Junos OS Configuration on page 360](#)
- [Overview of Junos OS CLI Operational Mode Commands on page 319](#)

**List of Sample Output** [show configuration on page 1549](#)  
[show configuration policy-options on page 1550](#)

**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 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 1607</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show chassis alarms on page 1551</a>
<b>Output Fields</b>	<a href="#">Table 228 on page 1551</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 228: show chassis alarms Output Fields**

Field Name	Field Description
Alarm time	Date and time the alarm was first recorded.
Class	Severity class for this alarm: Minor or Major.
Description	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 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*)  
     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.
- **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** [show interfaces Gigabit Ethernet on page 1562](#)

[show interfaces brief \(Gigabit Ethernet\) on page 1563](#)  
[show interfaces detail \(Gigabit Ethernet\) on page 1563](#)  
[show interfaces extensive \(Gigabit Ethernet\) on page 1565](#)  
[show interfaces terse on page 1568](#)  
[show interfaces controller \(Channelized E1 IQ with Logical E1\) on page 1568](#)  
[show interfaces controller \(Channelized E1 IQ with Logical DS0\) on page 1568](#)  
[show interfaces descriptions on page 1569](#)  
[show interfaces destination-class all on page 1569](#)  
[show interfaces diagnostics optics on page 1569](#)  
[show interfaces far-end-interval coc12-5/2/0 on page 1570](#)  
[show interfaces far-end-interval coc1-5/2/1:1 on page 1570](#)  
[show interfaces filters on page 1571](#)  
[show interfaces flow-statistics \(Gigabit Ethernet\) on page 1571](#)  
[show interfaces interval \(Channelized OC12\) on page 1572](#)  
[show interfaces interval \(E3\) on page 1572](#)  
[show interfaces interval \(SONET/SDH\) on page 1573](#)  
[show interfaces load-balancing on page 1573](#)  
[show interfaces load-balancing detail on page 1573](#)  
[show interfaces mc-ae on page 1574](#)  
[show interfaces media \(SONET/SDH\) on page 1574](#)  
[show interfaces policers on page 1574](#)  
[show interfaces policers interface-name on page 1575](#)  
[show interfaces queue on page 1575](#)  
[show interfaces redundancy on page 1576](#)  
[show interfaces redundancy \(Aggregated Ethernet\) on page 1576](#)  
[show interfaces redundancy detail on page 1576](#)  
[show interfaces routing brief on page 1576](#)  
[show interfaces routing detail on page 1577](#)  
[show interfaces routing-instance all on page 1577](#)  
[show interfaces snmp-index on page 1578](#)  
[show interfaces source-class all on page 1578](#)  
[show interfaces statistics \(Fast Ethernet\) on page 1578](#)  
[show interfaces switch-port on page 1579](#)  
[show interfaces transport pm on page 1579](#)

**Output Fields** [Table 229 on page 1555](#) lists the output fields for the **show interfaces** command. Output fields are listed in the approximate order in which they appear.

**Table 229: show interfaces Output Fields**

Field Name	Field Description	Level of Output
<b>Physical Interface</b>		
<b>Physical interface</b>	Name of the physical interface.	All levels
<b>Enabled</b>	State of the interface.	All levels
<b>Interface index</b>	Index number of the physical interface, which reflects its initialization sequence.	<b>detail extensive none</b>
<b>SNMP ifIndex</b>	SNMP index number for the physical interface.	<b>detail extensive none</b>

Table 229: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Link-level type	Encapsulation being used on the physical interface.	All levels
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
MTU	Maximum transmission unit size on the physical interface.	All levels
Link mode	Link mode: Full-duplex or Half-duplex.	
Speed	Speed at which the interface is running.	All levels
BPDU error	Bridge protocol data unit (BPDU) error: Detected or None	
Loopback	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
Source filtering	Source filtering status: <b>Enabled</b> or <b>Disabled</b> .	All levels
Flow control	Flow control status: <b>Enabled</b> or <b>Disabled</b> .	All levels
Auto-negotiation	(Gigabit Ethernet interfaces) Autonegotiation status: <b>Enabled</b> or <b>Disabled</b> .	All levels
Remote-fault	(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
Device flags	Information about the physical device.	All levels
Interface flags	Information about the interface.	All levels
Link flags	Information about the physical link.	All levels
CoS queues	Number of CoS queues configured.	detail extensive none
Current address	Configured MAC address.	detail extensive none
Last flapped	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> .	detail extensive none
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None
Output Rate	Output rate in bps and pps.	None

Table 229: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Active alarms and Active defects</b>	<p>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. These fields can contain the value <b>None</b> or <b>Link</b>.</p> <ul style="list-style-type: none"> <li>• <b>None</b>—There are no active defects or alarms.</li> <li>• <b>Link</b>—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</li> </ul>	<b>detail extensive none</b>
<b>Statistics last cleared</b>	Time when the statistics for the interface were last set to zero.	<b>detail extensive</b>
<b>Traffic statistics</b>	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes</b>—Number of bytes received on the interface.</li> <li>• <b>Output bytes</b>—Number of bytes transmitted on the interface.</li> <li>• <b>Input packets</b>—Number of packets received on the interface.</li> <li>• <b>Output packets</b>—Number of packets transmitted on the interface.</li> </ul>	<b>detail extensive</b>
<b>Input errors</b>	<p>Input errors on the interface.</p> <ul style="list-style-type: none"> <li>• <b>Errors</b>—Sum of the incoming frame aborts and FCS errors.</li> <li>• <b>Drops</b>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</li> <li>• <b>Framing errors</b>—Number of packets received with an invalid frame checksum (FCS).</li> <li>• <b>Runts</b>—Number of frames received that are smaller than the runt threshold.</li> <li>• <b>Policed discards</b>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</li> <li>• <b>L3 incompletes</b>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <b>ignore-l3-incompletes</b> statement.</li> <li>• <b>L2 channel errors</b>—Number of times the software did not find a valid logical interface for an incoming frame.</li> <li>• <b>L2 mismatch timeouts</b>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</li> <li>• <b>FIFO errors</b>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</li> <li>• <b>Resource errors</b>—Sum of transmit drops.</li> </ul>	<b>extensive</b>

Table 229: 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 229: 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 229: show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Filter statistics</b>	<p><b>Receive</b> and <b>Transmit</b> 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>	<b>extensive</b>
<b>Autonegotiation information</b>	<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>	<b>extensive</b>
<b>Packet Forwarding Engine configuration</b>	<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>	<b>extensive</b>

Table 229: 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 229: 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:

```

Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use

Queue counters:            Queued packets    Transmitted packets            Dropped packets

0 best-effort                            0                            0                            0

1 expedited-fo                            0                            0                            0

2 assured-forw                            0                            0                            0

3 network-cont                            0                            0                            0

Queue number:            Mapped forwarding classes

0                            best-effort

1                            expedited-forwarding

2                            assured-forwarding

3                            network-control

Active alarms : LINK

Active defects : LINK

MAC statistics:                            Receive                            Transmit

Total octets                            0                            0

Total packets                            0                            0

Unicast packets                            0                            0

Broadcast packets                            0                            0

Multicast packets                            0                            0

CRC/Align errors                            0                            0

FIFO errors                            0                            0

MAC control frames                            0                            0

MAC pause frames                            0                            0

Oversized frames                            0

Jabber frames                            0

Fragment frames                            0

VLAN tagged frames                            0

Code violations                            0

Filter statistics:

Input packet count                            0

Input packet rejects                            0

Input DA rejects                            0

Input SA rejects                            0

Output packet count                            0

Output packet pad count                            0

Output packet error count                            0

CAM destination filters: 2, CAM source filters: 0

Autonegotiation information:

Negotiation status: Incomplete

Packet Forwarding Engine configuration:

Destination slot: 0

CoS information:

Direction : Output

CoS transmit queue                            Bandwidth                            Buffer Priority

Limit                            %                            bps                            %                            usec                            low

0 best-effort                            95                            950000000                            95                            0                            low

none

3 network-control                            5                            50000000                            5                            0                            low

none

Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)



```

Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
Security: Zone: public
Flow Statistics :
Flow Input statistics :
  Self packets : 0
  ICMP packets : 0
  VPN packets : 0
  Multicast packets : 0
  Bytes permitted by policy : 0
  Connections established : 0
Flow Output statistics:
  Multicast packets : 0
  Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
  Address spoofing: 0
  Authentication failed: 0
  Incoming NAT errors: 0
  Invalid zone received packet: 0
  Multiple user authentications: 0
  Multiple incoming NAT: 0
  No parent for a gate: 0
  No one interested in self packets: 0
  No minor session: 0
  No more sessions: 0
  No NAT gate: 0
  No route present: 0
  No SA for incoming SPI: 0
  No tunnel found: 0
  No session for a gate: 0
  No zone or NULL zone binding: 0
  Policy denied: 0
  Security association not active: 0
  TCP sequence number out of window: 0
  Syn-attack protection: 0
  User authentication errors: 0
Protocol inet, MTU: 1500, Generation: 150, Route table: 0
Flags: Sendbcst-pkt-to-re
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255,
  Generation: 150

```

## Sample Output

### show interfaces terse

```

user@host> show interfaces terse

```

Interface	Admin	Link	Proto	Local	Remote
ge-0/0/0	up	up			
ge-0/0/0.0	up	up	inet	10.209.4.61/18	
gr-0/0/0	up	up			
ip-0/0/0	up	up			
st0	up	up			
st0.1	up	ready	inet		
ls-0/0/0	up	up			
lt-0/0/0	up	up			
mt-0/0/0	up	up			
pd-0/0/0	up	up			
pe-0/0/0	up	up			
e3-1/0/0	up	up			
t3-2/0/0	up	up			
e1-3/0/0	up	up			
se-4/0/0	up	down			
t1-5/0/0	up	up			
br-6/0/0	up	up			
dc-6/0/0	up	up			
dc-6/0/0.32767	up	up			
bc-6/0/0:1	down	up			
bc-6/0/0:1.0	up	down			
d10	up	up			
d10.0	up	up	inet		
dsc	up	up			
gre	up	up			
ipip	up	up			
lo0	up	up			
lo0.16385	up	up	inet	10.0.0.1 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 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		
			iso		
gr-0/3/0	up	up			
ip-0/3/0	up	up			
mt-0/3/0	up	up			
pd-0/3/0	up	up			
pe-0/3/0	up	up			
...					
so-2/0/0	up	up			



```

so-2/0/0.0      up    up    inet  so-2/0/0.0-in-policer so-2/0/0.0-out-policer
                  iso
so-2/1/0        up    down
...

```

### show interfaces policers interface-name

```

user@host> show interfaces policers so-2/1/0
Interface      Admin Link Proto Input Policer      Output Policer
so-2/1/0       up    down
so-2/1/0.0     up    down inet  so-2/1/0.0-in-policer so-2/1/0.0-out-policer
                  iso
                  inet6

```

## Sample Output

### show interfaces queue

The following truncated example shows the CoS queue sizes for queues 0, 1, and 3. Queue 1 has a queue buffer size (guaranteed allocated memory) of 9192 bytes.

```

user@host> show interfaces queue
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 134, SNMP ifIndex: 509
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: class0
  Queued:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
  Transmitted:
    Packets      :                0                0 pps
    Bytes        :                0                0 bps
    Tail-dropped packets :                0                0 pps
    RL-dropped packets  :                0                0 pps
    RL-dropped bytes    :                0                0 bps
    RED-dropped packets :                0                0 pps
    Low               :                0                0 pps
    Medium-low        :                0                0 pps
    Medium-high       :                0                0 pps
    High              :                0                0 pps
    RED-dropped bytes  :                0                0 bps
    Low               :                0                0 bps
    Medium-low        :                0                0 bps
    Medium-high       :                0                0 bps
    High              :                0                0 bps
  Queue Buffer Usage:
    Reserved buffer    :                118750000 bytes
    Queue-depth bytes  :
    Current            :                0
  ..
  ..
Queue: 1, Forwarding classes: class1
  ..
  ..
  Queue Buffer Usage:
    Reserved buffer    :                9192 bytes
    Queue-depth bytes  :
    Current            :                0
  ..

```

```

..
Queue: 3, Forwarding classes: class3
  Queued:
..
..
Queue Buffer Usage:
  Reserved buffer      :          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:
    Receive      Transmit
    Total bytes  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 PM	Suspect Flag:True	Reason:Unknown		
	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 PM	Suspect Flag:False	Reason:None		
	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 PM	Suspect Flag:True	Reason:Unknown		
	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 PM	Suspect Flag:False	Reason:None		
	COUNT	THRESHOLD	TCA-ENABLED	TCA-RAISED
FEC-CorrectedErr	2008544300	0	NA	NA
FEC-UncorrectedWords	0	0	NA	NA
BER PM	Suspect Flag:False	Reason:None		
	MIN	MAX	AVG	THRESHOLD
TCA-RAISED				TCA-ENABLED
BER	3.6e-5	5.8e-5	3.6e-5	10.0e-3
Yes				No
Physical interface: et-0/1/0, SNMP ifIndex 515				
14:45-current				
PM	Suspect Flag:True	Reason:Object Disabled		
	CURRENT	MIN	MAX	AVG
TCA-ENABLED	TCA-RAISED			
				(MIN)
(MAX)	(MIN)	(MAX)	(MIN)	(MAX)
Lane chromatic dispersion	0	0	0	0
0	NA	NA	NA	NA
Lane differential group delay	0	0	0	0
0	NA	NA	NA	NA
q Value	120	120	120	120
0	NA	NA	NA	NA
SNR	28	28	29	28
0	NA	NA	NA	NA
Tx output power(0.01dBm)	-5000	-5000	-5000	-5000
-100	No	No	No	No
Rx input power(0.01dBm)	-3642	-3665	-3626	-3637
-500	No	No	No	No
Module temperature(Celsius)	46	46	46	46
75	No	No	No	No
Tx laser bias current(0.1mA)	0	0	0	0
0	NA	NA	NA	NA
Rx laser bias current(0.1mA)	1270	1270	1270	1270
0	NA	NA	NA	NA
Carrier frequency offset(MHz)	-186	-186	-186	-186
5000	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>Ethernet Interfaces Feature Guide for Security Devices</i></li> <li><i>Example: Configuring PoE on All Interfaces</i></li> </ul>
<b>Output Fields</b>	Table 230 on page 1582 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 230: 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 interface (View)

<b>Syntax</b>	show poe telemetries interface ge-fpc/pic/port all   x
<b>Release Information</b>	Command introduced in Release 9.5 of Junos OS.
<b>Description</b>	Display a history of power consumption on the specified interface.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>ge-fpc/pic/port</b>—Display telemetries for the specified PoE interface.</li> <li>• <b>all</b>—Display all telemetries records for the specified PoE interface.</li> <li>• <b>x</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>Ethernet Interfaces Feature Guide for Security Devices</i></li> <li>• <i>Example: Configuring PoE on All Interfaces</i></li> </ul>
<b>Output Fields</b>	Table 231 on page 1584 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 231: 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 all
```

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 interface ge-0/0/1 5
```

Sl 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>	For SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices, statement introduced in Release 9.5 of Junos OS.
<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>Junos OS Interfaces Library for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show pppoe interfaces on page 1588</a> <a href="#">show pppoe interfaces brief on page 1588</a> <a href="#">show pppoe interfaces detail on page 1588</a> <a href="#">show pppoe interfaces extensive on page 1588</a>
<b>Output Fields</b>	Table 232 on page 1586 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 232: show pppoe interfaces Output Fields

Field Name	Field Description
<b>Index</b>	Index number of the logical interface, which reflects its initialization sequence.
<b>State</b>	State of the logical interface: <b>up</b> or <b>down</b> .
<b>Session ID</b>	Session ID.
<b>Service name</b>	Type of service required (can be used to indicate an ISP name, a class, or quality of service).
<b>Configured AC name</b>	Configured access concentrator name.

Table 232: show pppoe interfaces Output Fields (*continued*)

Field Name	Field Description
<b>Session AC name</b>	Name of the access concentrator.
<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>	For SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 devices, statement introduced in Release 9.5 of Junos OS.
<b>Description</b>	Display statistics information about PPPoE interfaces.
<b>Options</b>	<b>none</b> —Display PPPoE statistics for all interfaces.  <i>logical-interface-name</i> —(Optional) Name of an underlying PPPoE logical interface.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show pppoe interfaces on page 1586</a></li> <li><i>Junos OS Interfaces Library for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show pppoe statistics on page 1591</a>
<b>Output Fields</b>	<a href="#">Table 233 on page 1590</a> 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 233: 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 233: 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*
- *Security Policies Feature Guide for Security Devices*

**List of Sample Output**

[show security alarms on page 1594](#)  
[show security alarms detail on page 1594](#)  
[show security alarms alarm-id on page 1594](#)  
[show security alarms alarm-type authentication on page 1594](#)  
[show security alarms newer-than <time> on page 1595](#)  
[show security alarms older-than <time> on page 1595](#)  
[show security alarms process <process> on page 1595](#)  
[show security alarms severity <severity> on page 1595](#)

**Output Fields** [Table 234 on page 1593](#) 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 234: 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 234: 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 1597</a></li> <li>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security datapath—debug capture on page 1596</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 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 1596</a></li> <li>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security datapath-debug counter on page 1597</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>List of Sample Output</b>	<a href="#">show security monitoring fpc 0 on page 1599</a> <a href="#">show security monitoring fpc 1 on page 1599</a> <a href="#">show security monitoring fpc 8 on page 1599</a>
<b>Output Fields</b>	<a href="#">Table 235 on page 1598</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 235: 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).
Current flow session	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.



Table 235: show security monitoring fpc fpc-number Output Fields (*continued*)

Field Name	Field Description
Max flow session	The maximum number of flow sessions allowed. This number will differ from one device to another.
SPU current cp session	The current number of cp sessions for the SPU (on SRX3400, SRX3600, SRX5600, and SRX5800 devices only).
SPU max cp session	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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

## 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**

- *Network Monitoring and Troubleshooting Guide for Security Devices*

## 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 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><i>IP Monitoring Feature Guide for Security Devices</i></li> <li><i>show services ip-monitoring status</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show services rpm probe-results on page 1606</a>
<b>Output Fields</b>	<a href="#">Table 236 on page 1603</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 236: 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 236: 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 236: 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 1607</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 1608](#)  
                               [Syntax \(QFX Series\) on page 1608](#)

**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 1610](#)  
[traceroute as-number-lookup host on page 1610](#)  
[traceroute no-resolve on page 1610](#)  
[traceroute propagate-ttl on page 1611](#)  
[traceroute \(Between CE Routers, Layer 3 VPN\) on page 1611](#)  
[traceroute \(Through an MPLS LSP\) on page 1611](#)

**Output Fields** [Table 237 on page 1610](#) describes the output fields for the **traceroute** command. Output fields are listed in the approximate order in which they appear.

**Table 237: 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  mpls5-1o0.company.net (10.168.1.224)  0.420 ms  0.394 ms  0.401 ms

```

## Troubleshooting

- [Troubleshooting Security Devices on page 1611](#)

### Troubleshooting Security Devices

- [Recovering the Root Password for J Series Devices on page 1612](#)
- [Recovering the Root Password for SRX Series Devices on page 1614](#)
- [Troubleshooting Access Manager Client-Side Problems on page 1615](#)
- [Troubleshooting DNS Name Resolution in Logical System Security Policies on page 1616](#)
- [Troubleshooting the Link Services Interface on page 1616](#)
- [Troubleshooting Security Policies on page 1625](#)
- [Troubleshooting the TGM550 Module and VoIP Interface on page 1627](#)
- [Troubleshooting ISSU-Related Problems Using Log Error Messages on page 1628](#)

## Recovering the Root Password for J Series Devices

If you forget the root password for the device, you can use the password recovery procedure to reset the root password.

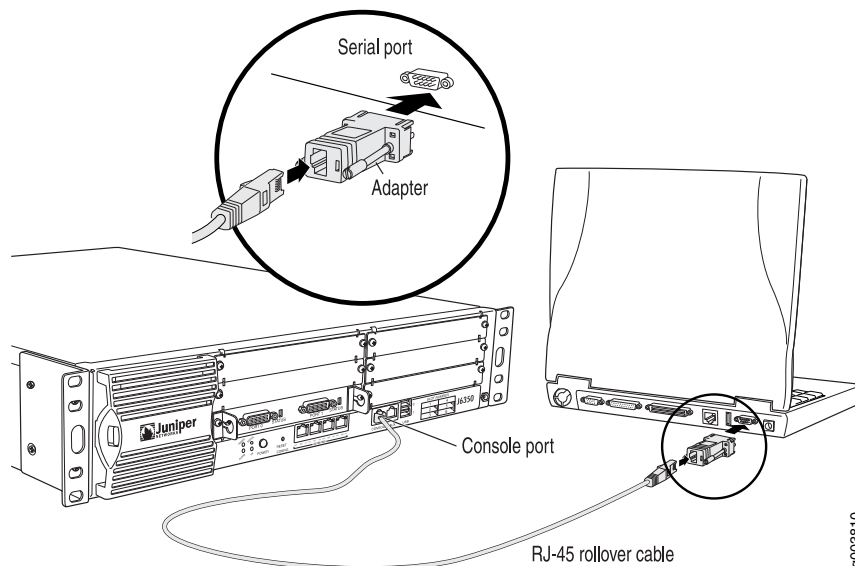


**NOTE:** You need console access to recover the root password.

To recover the root password for a J Series device:

1. Power off the device by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the device into the RJ-45 to DB-9 serial port adapter supplied with the device (see [Figure 56 on page 1612](#)).
4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see [Figure 56 on page 1612](#)).
5. Connect the other end of the Ethernet rollover cable to the console port on the device (see [Figure 56 on page 1612](#)).

**Figure 56: Connecting to the Console Port on the J Series Device**



6. Turn on the power to the management device.
7. Connect a management device, such as a PC or laptop computer, to the console port on the device.
8. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
9. Configure the port settings as follows:

- Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
10. 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.

11. Press the Spacebar to access the device's bootstrap loader command prompt:

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
```

12. Enter **boot -s** to start up the system in single-user mode.

```
ok boot -s
```

13. Enter **recovery** to start the root password recovery procedure.

```
Enter full pathname of shell or 'recovery' for root password recovery or
RETURN for /bin/sh: recovery
```

14. Enter configuration mode in the CLI.

15. Set the root password.

```
user@host# set system root-authentication plain-text-password
```

16. Enter the new root password.

```
New password: juniper1
Retype new password:
```

17. At the second prompt, reenter the new root password.

18. If you are finished configuring the network, commit the configuration.

```
root@host# commit
commit complete
```

19. Exit from configuration mode.

20. Exit from operational mode.

21. At the prompt, enter **y** to reboot the router.

```
Reboot the system? [y/n] y
```

#### Related Documentation

- [Recovering the Root Password for SRX Series Devices on page 1614](#)
- [System Log Messages](#)
- *Network Monitoring and Troubleshooting Guide for Security Devices*

## 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**
- [Recovering the Root Password for J Series Devices on page 1612](#)
  - [System Log Messages](#)
  - *Network Monitoring and Troubleshooting Guide for Security Devices*

### 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*
  - *Dynamic VPN Feature Guide for SRX Series Gateway Devices*

### Troubleshooting DNS Name Resolution in Logical System Security Policies

**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*
- *show security dns-cache*
- *clear security dns-cache*
- [show security policies on page 109](#)
- *Master Administrator for Logical Systems Feature Guide for Security Devices*

### 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 1617](#)
- [Determine What Causes Jitter and Latency on the Multilink Bundle on page 1618](#)
- [Determine If LFI and Load Balancing Are Working Correctly on page 1618](#)
- [Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device on page 1625](#)

***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 238 on page 1617 shows the CoS components to be applied on a multilink bundle and its constituent links.

**Table 238: 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>

Table 238: CoS Components Applied on Multilink Bundles and Constituent Links (*continued*)

Cos Component	Multilink Bundle	Constituent Links	Explanation
Shaping rate for a per-unit scheduler or an interface-level scheduler	No	Yes	Because per-unit scheduling is applied only at the end point, apply this shaping rate to the constituent links only. Any configuration applied earlier is overwritten by the constituent link configuration.
Transmit-rate exact or queue-level shaping	Yes	No	The interface-level shaping applied on the constituent links overrides any shaping on the queue. Thus apply transmit-rate exact shaping on the multilink bundle only.
Rewrite rules	Yes	No	Rewrite bits are copied from the packet into the fragments automatically during fragmentation. Thus what you configure on the multilink bundle is carried on the fragments to the constituent links.
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.

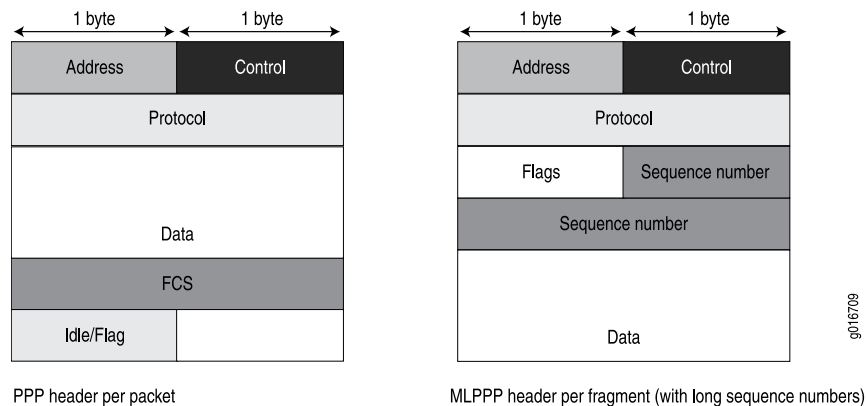
A small unfragmented data packet contains a PPP header and a single MLPPP header. In a large fragmented data packet, the first fragment contains a PPP header and an MLPPP header, but the consecutive fragments contain only an MLPPP header.

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 57 on page 1621 shows the overhead added to PPP and MLPPP headers.

**Figure 57: 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 239 on page 1621 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 239: 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 239: 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 240 on page 1624](#) 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 240: 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.

#### ***Determine Why Packets Are Dropped on a PVC Between a Juniper Networks Device and a Third-Party Device***

**Problem Description:** You are configuring a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces on a Juniper Networks device and a third-party device, and packets are being dropped and ping fails.

**Solution** If the third-party device does not have the same FRF.12 support as the Juniper Networks device or supports FRF.12 in a different way, the Juniper Networks device interface on the PVC might discard a fragmented packet containing FRF.12 headers and count it as a "Policed Discard."

As a workaround, configure multilink bundles on both peers, and configure fragmentation thresholds on the multilink bundles.

---

### **Troubleshooting Security Policies**

- [Synchronizing Policies Between Routing Engine and Packet Forwarding Engine on page 1625](#)
- [Checking a Security Policy Commit Failure on page 1626](#)
- [Verifying a Security Policy Commit on page 1626](#)
- [Debugging Policy Lookup on page 1627](#)

#### ***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 1625](#)
- [Checking a Security Policy Commit Failure on page 1626](#)
- [Verifying a Security Policy Commit on page 1626](#)
- [Debugging Policy Lookup on page 1627](#)
- *Security Policies Feature Guide for Security Devices*

---

### ***Troubleshooting the TGM550 Module and VoIP Interface***

**Problem Description:** The TGM550 module is installed but the VoIP interface is unavailable. The TGM550 module is installed and the VoIP interface—for example, `vp-3/0/0` is configured, but the interface is not accessible. The **show chassis hardware** command displays the TGM550 installed on slot 3. However, the **show interfaces terse** command does not display the `vp-3/0/0` interface, and the **show interfaces vp-3/0/0** command displays an error:

```
user@host> show interfaces vp-3/0/0
error: device vp-3/0/0 not found
```

**Solution**      The VoIP interface might be unavailable because the TGM550 firmware version is not compatible with the Junos OS version installed on the device.

To correct the TGM550 firmware and Junos OS version compatibility error:

1. Check the router's system log messages for a version incompatibility error similar to the following:  

```
Jan 5 11:07:03 host fwdd[2857]: TGMT: RE (1.0) - TGM (2.0) major protocol version mismatch: not marking TGM slot ready
```
2. If the error exists, connect to the TGM550 through the console port.
3. View the TGM550 firmware version.

```
TGM550-003(super)# show image version
Bank      Version
-----
A (current) 26.23.0
B          26.22.0
```

In this example, the current TGM550 firmware version is **26.23.0**.

4. Identify the Junos OS version that is compatible with the current TGM550 firmware version.
5. Upgrade the router with the compatible Junos OS version.

**Related Documentation**

- *Communication Manager Software & Firmware Compatibility Matrix* at <http://support.avaya.com>
- *Avaya VoIP Modules Overview*
- *Avaya VoIP Modules Configuration Overview*
- *Understanding the TGM550 Telephony Gateway Module*
- *Avaya IG550 Integrated Gateway Overview*
- *Example: Configuring VoIP Interfaces*

---

### 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 1628](#)
- [Kernel State Synchronization on page 1628](#)
- [Installation Related Errors on page 1629](#)
- [ISSU Support Related Errors on page 1629](#)
- [RG Groups Failover Errors on page 1629](#)
- [Initial Validation Checks Fail on page 1629](#)

#### ***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*



## CHAPTER 19

# System Log Monitoring and Troubleshooting Guide for Security Devices

- [Overview on page 1633](#)
- [Configuration on page 1647](#)
- [Administration on page 1696](#)

### Overview

---

- [System Log Messages on page 1633](#)
- [Security Devices on page 1643](#)
- [Single-Chassis Systems on page 1646](#)

### System Log Messages

- [Junos OS System Log Configuration Overview on page 1633](#)
- [Junos OS Platform-Specific Default System Log Messages on page 1634](#)
- [Displaying and Interpreting System Log Message Descriptions on page 1635](#)
- [Interpreting Messages Generated in Structured-Data Format on page 1636](#)
- [Interpreting Messages Generated in Standard Format by Services on a PIC on page 1641](#)
- [Junos OS System Logging Facilities and Message Severity Levels on page 1642](#)

#### [Junos OS System Log Configuration Overview](#)

---

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the router, 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 1655](#)

### 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 1655.

- On J Series routers, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

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 Configuration Overview on page 1633](#)

- [Junos OS Default System Log Settings on page 1656](#)

### Displaying and Interpreting System Log Message Descriptions

The *Junos OS System Log 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 241 on page 1635](#) describes the fields in a system log message description in this reference or in the CLI.

**Table 241: 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 Name field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error.</p>

Table 241: Fields in System Log Message Descriptions (*continued*)

Field Name in Reference	Field Name in CLI	Description
—	<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>	Category to which the message belongs: <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>
<b>Severity</b>	<b>Severity</b>	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> .
<b>Cause</b>	<b>Cause</b>	(Optional) Possible cause for message generation. There can be more than one cause.
<b>Action</b>	<b>Action</b>	(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 1659](#).

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 242 on page 1637 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen ( - ) appears instead.

**Table 242: 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 in Specifying the Facility and Severity of Messages to Include in the Log.</b>	<165> for a message from the pfe facility (facility=20) with severity notice (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

Table 242: Fields in Structured-Data Messages (*continued*)

Field	Description	Examples
<code>junos@2636.platform</code>	An identifier for the type of hardware platform that generated the message. The <code>junos@2636</code> 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 244 on page 1640</a> .	<code>junos@2636.1.1.1.2.18</code> for the M120 router
<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</i> = " <i>value</i> ".	<code>username="user"</code>
<i>message-text</i>	English-language description of the event or error (omitted if the brief statement is included at the <code>[edit system syslog file <i>filename</i> structured-data]</code> 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 243 on page 1638](#) 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 243 on page 1638](#) 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 243: 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



Table 243: Facility and Severity Codes in the priority-code Field (*continued*)

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
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
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 244 on page 1640 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 *SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices*.

**Table 244: 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

Table 244: Platform Identifiers in the platform Field (*continued*)

Identifier	Platform Name
1.1.1.2.83	T4000 router

### 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 245 on page 1641 describes the message fields.

Table 245: 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.
<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.

Table 245: Fields in Messages Generated by a PIC (*continued*)

Field	Description
<b>message-text</b>	Text of the message. For the text of each message, see System Log Messages.

### Junos OS System Logging Facilities and Message Severity Levels

Table 246 on page 1642 lists the Junos system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 246: 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 247 on page 1643 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 1666.

Table 247: 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 1647](#)

## Security Devices

- [Understanding System Logging for Security Devices on page 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)

### 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 1643](#)
- [Control Plane and Data Plane Logs on page 1644](#)

#### **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 J Series devices, the most common logging configuration is the Junos OS configuration in which 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.
  - 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 may 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 1645](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)
- [Sending System Log Messages to a File on page 1652](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

---

**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 1651](#)
- [Understanding System Logging for Security Devices on page 1643](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)

- [Sending System Log Messages to a File on page 1652](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

## Single-Chassis Systems

- [Displaying a Log File from a Single-Chassis System on page 1646](#)
- [The message-source Field on a Single-Chassis System on page 1646](#)

---

### 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 log log-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
```

#### Related Documentation

- [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 1641](#)
- [Interpreting Messages Generated in Structured-Data Format on page 1636](#)
- [Examples: Displaying a Log File on page 1649](#)

---

### 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).

## Configuration

---

- [System Log Messages on page 1647](#)
- [Security Devices on page 1651](#)
- [Single-Chassis Systems on page 1654](#)
- [Configuration Statements on page 1666](#)

## System Log Messages

- [Examples: Configuring System Logging on page 1647](#)
- [Examples: Assigning an Alternative Facility on page 1649](#)
- [Examples: Displaying a Log File on page 1649](#)
- [Examples: Displaying System Log Message Descriptions on page 1650](#)

### 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*

### 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*

### 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
```

### 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

```

## Security Devices

- [Configuring Binary Security Log Files on page 1651](#)
- [Sending System Log Messages to a File on page 1652](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)

### 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 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)
- [Sending System Log Messages to a File on page 1652](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

### 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 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

### 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 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)

- [Setting the System to Stream Security Logs Through Revenue Ports on page 1654](#)
- [Sending System Log Messages to a File on page 1652](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

### 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 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)
- [Setting the System to Send All Log Messages Through eventd on page 1653](#)
- [Sending System Log Messages to a File on page 1652](#)
- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

### Single-Chassis Systems

- [Junos OS Minimum System Logging Configuration on page 1655](#)
- [Junos OS Default System Log Settings on page 1656](#)



- [Junos OS Platform-Specific Default System Log Messages on page 1657](#)
- [Specifying the Facility and Severity of Messages to Include in the Log on page 1658](#)
- [Directing System Log Messages to a Log File on page 1658](#)
- [Logging Messages in Structured-Data Format on page 1659](#)
- [Directing System Log Messages to a User Terminal on page 1660](#)
- [Directing System Log Messages to the Console on page 1660](#)
- [System Log Default Facilities for Messages Directed to a Remote Destination on page 1660](#)
- [Adding a Text String to System Log Messages on page 1661](#)
- [Adding a String on page 1662](#)
- [Including Priority Information in System Log Messages on page 1662](#)
- [Including the Year or Millisecond in Timestamps on page 1663](#)
- [Using Regular Expressions to Refine the Set of Logged Messages on page 1664](#)
- [Disabling the System Logging of a Facility on page 1666](#)

### 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 248 on page 1655](#). For more information about the configuration statements, see *Single-Chassis System Logging Configuration Overview*.

**Table 248: 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>
Router or switch console	<pre>[edit system syslog] console {   facility severity; }</pre>
Remote machine or the other Routing Engine on the router or switch	<pre>[edit system syslog] host (hostname   other-routing-engine) {   facility severity; }</pre>

#### Related Documentation

- [Junos OS System Log Configuration Overview on page 1633](#)

## Junos OS Default System Log Settings

Table 249 on page 1656 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 249: 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	[edit system syslog] host <i>hostname</i> { facility-override <i>facility</i> ; }	<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	[edit system syslog] file <i>filename</i> { structured-data; }	<a href="#">“Logging Messages in Structured-Data Format” on page 1659</a>
Maximum number of files in the archived set	10	[edit system syslog] archive { files <i>number</i> ; } file <i>filename</i> { archive { files <i>number</i> ; } }	<i>Specifying Log File Size, Number, and Archiving Properties</i>
Maximum size of the log file	J Series: 128 kilobytes (KB)  M Series, MX Series, and T Series: 1 megabyte (MB)  TX Matrix: 10 MB	[edit system syslog] archive { size <i>size</i> ; } file <i>filename</i> { archive { size <i>size</i> ; } }	<i>Specifying Log File Size, Number, and Archiving Properties</i>
Timestamp format	Month, date, hour, minute, second  For example: Aug 21 12:36:30	[edit system syslog] time-format <i>format</i> ;	<a href="#">“Including the Year or Millisecond in Timestamps” on page 1663</a>

Table 249: Default System Logging Settings (*continued*)

Setting	Default	Overriding Statement	Instructions
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 <i>filename</i> {   archive {     world-readable;   } }</pre>	<i>Specifying Log File Size, Number, and Archiving Properties</i>

- [Junos OS System Log Configuration Overview on page 1633](#)
- [Junos OS Platform-Specific Default System Log Messages on page 1634](#)

### 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 1655.

- On J Series routers, a message is logged when a process running in the kernel consumes 500 or more consecutive milliseconds of CPU time.

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 Configuration Overview on page 1633](#)
  - [Junos OS Default System Log Settings on page 1656](#)

### 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 1642](#)
  - [Single-Chassis System Logging Configuration Overview](#)
  - [Examples: Configuring System Logging on page 1647](#)

### 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” on page 1658](#).

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 1662
- **match**—See “Using Regular Expressions to Refine the Set of Logged Messages” on page 1664
- **structured-data**—See “Logging Messages in Structured-Data Format” on page 1659

#### Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- [Examples: Configuring System Logging on page 1647](#)

### 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. .

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 1647](#)

## 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” on page 1658](#). For information about the **match** statement, see [“Using Regular Expressions to Refine the Set of Logged Messages” on page 1664](#).

### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1647](#)

## 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” on page 1658](#).

### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1647](#)

## System Log Default Facilities for Messages Directed to a Remote Destination

[Table 250 on page 1660](#) 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 250: Default Facilities for Messages Directed to a Remote Destination**

Junos OS-specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6

**Table 250: Default Facilities for Messages Directed to a Remote Destination (*continued*)**

Junos OS—specific Local Facility	Default Facility When Directed to Remote Destination
<b>conflict-log</b>	<b>local5</b>
<b>dfc</b>	<b>local1</b>
<b>firewall</b>	<b>local3</b>
<b>interactive-commands</b>	<b>local7</b>
<b>pfe</b>	<b>local4</b>

**Related Documentation**

- *Single-Chassis System Logging Configuration Overview*

**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'
```

### 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 1659](#).

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.)

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
```

#### Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- [Examples: Configuring System Logging on page 1647](#)

#### 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 1659](#).

#### Related Documentation

- [Single-Chassis System Logging Configuration Overview](#)
- [Examples: Configuring System Logging on page 1647](#)

### 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 251 on page 1665](#) 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 251: 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 1647](#)

---

### 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](#)

## Configuration Statements

- [allow-duplicates on page 1668](#)
- [archive \(All System Log Files\) on page 1669](#)
- [cache \(Security Log\) on page 1670](#)
- [console \(System Logging\) on page 1671](#)
- [destination-override on page 1672](#)
- [event-rate on page 1672](#)
- [explicit-priority on page 1673](#)
- [exclude \(Security Log\) on page 1674](#)
- [facility-override on page 1675](#)
- [file \(Security Log\) on page 1676](#)
- [file \(System Logging\) on page 1677](#)

- [files](#) on page 1678
- [host \(Security Log\)](#) on page 1679
- [limit \(Security Log\)](#) on page 1679
- [log \(Services\)](#) on page 1680
- [log-prefix](#) on page 1681
- [log-rotate-frequency](#) on page 1681
- [match](#) on page 1682
- [mode \(Security Log\)](#) on page 1682
- [no-remote-trace](#) on page 1682
- [pic-services-logging](#) on page 1683
- [port](#) on page 1684
- [security-log](#) on page 1685
- [security-log-percent-full](#) on page 1685
- [severity \(Security Log\)](#) on page 1686
- [size](#) on page 1687
- [system](#) on page 1687
- [structured-data](#) on page 1688
- [syslog](#) on page 1689
- [time-format](#) on page 1691
- [traceoptions \(Security Log\)](#) on page 1692
- [tracing](#) on page 1694
- [user \(System Logging\)](#) on page 1695
- [world-readable](#) on page 1696

## 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>	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 Log Monitoring and Troubleshooting Guide for Security Devices</i></li></ul>

## archive (All System Log Files)

<b>Syntax</b>	<code>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;world-readable   no-world-readable&gt; ;</code>
<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 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><i>logfile</i></b>, it closes the file, compresses it, and renames it <b><i>logfile.0.gz</i></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><i>logfile</i></b>. When the new file reaches the maximum size, the <b><i>logfile.0.gz</i></b> file is renamed to <b><i>logfile.1.gz</i></b>, and the new file is closed, compressed, and renamed <b><i>logfile.0.gz</i></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><i>logfile</i></b> before archiving it (closing it, compressing it, and changing its name to <b><i>logfile.0.gz</i></b>). The utility then opens and writes to a new file called <b><i>logfile</i></b>.</p> <p><b>Syntax:</b> <b><i>xk</i></b> to specify the number of kilobytes, <b><i>xm</i></b> for the number of megabytes, or <b><i>xg</i></b> for the number of gigabytes</p> <p><b>Range:</b> 64 KB through 1 GB</p> <p><b>Default:</b> 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers</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>
<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> </ul>

## cache (Security Log)

---

**Syntax**    `cache {  
              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-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.

**Required Privilege Level**    security—To view this statement in the configuration.  
                                  security-control—To add this statement to the configuration.

**Related Documentation**

- *System Log Monitoring and Troubleshooting Guide for Security Devices*



## 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 246 on page 1642</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 247 on page 1643</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 1660</a></li><li>• <i>Junos OS System Log Reference</i></li></ul>

## destination-override

---

<b>Syntax</b>	<code>destination-override {     syslog host <i>ip-address</i>; }</code>
<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>	<p>These options specify the system logs and the host to which remote tracing output is sent:</p> <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>	<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="#">tracing on page 1694</a></li></ul>

## event-rate

---

<b>Syntax</b>	<code>Syntax event-rate <i>rate</i></code>
<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.
<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>

## 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 1662</a></li><li>• <i>Junos OS System Log Reference</i></li><li>• <a href="#">structured-data on page 1688</a></li></ul>

## exclude (Security Log)

---

Syntax	<pre>exclude <i>exlude-name</i> {     destination-address <i>destination-address</i>;     destination-port <i>destination-port</i>;     event-id <i>event-id</i>;     failure;     interface-name <i>interface-name</i>;     policy-name <i>policy-name</i>;     process <i>process-name</i>;     protocol <i>protocol</i>;     source-address <i>source-address</i>;     source-port <i>source-port</i>;     success;     user-name <i>user-name</i>; }</pre>
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	<ul style="list-style-type: none"><li>• <b>destination-ip</b> <i>destination-address</i>—Destination IP address.</li><li>• <b>destination-port</b> <i>destination-port</i>—Destination port number.</li><li>• <b>event-id</b> <i>event-id</i>—Error message identification number.</li><li>• <b>failure</b>—Failed audit event logs.</li><li>• <b>interface-name</b> <i>interface-name</i>—Name of the interface.</li><li>• <b>policy-name</b> <i>policy-name</i>—Policy name filter.</li><li>• <b>process</b> <i>process-name</i>—Process that generated the event.</li><li>• <b>protocol</b> <i>protocol</i>—Protocol that generated the event.</li><li>• <b>source-ip</b> <i>source-address</i>—Source IP address.</li><li>• <b>source-port</b> <i>source-port</i>—Source port number.</li><li>• <b>success</b>—Successful audit event logs.</li><li>• <b>username</b> <i>user-name</i>—User name filter.</li></ul>
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"><li>• <a href="#">show security log on page 1709</a></li><li>• <a href="#">clear security log on page 1700</a></li></ul>

## facility-override

---

<b>Syntax</b>	<code>facility-override <i>facility</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>	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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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 246 on page 1642</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 247 on page 1643</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 1658</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 1687</a></li></ul>



## host (Security Log)

---

<b>Syntax</b>	host { <code>ip-address</code> ; port <code>port-number</code> ; }
<b>Hierarchy Level</b>	[edit security log stream <i>stream-name</i> ]
<b>Release Information</b>	Statement introduced in Release 9.2 of Junos OS.
<b>Description</b>	You can specify the IP address of the server to which the security logs will be streamed.
<b>Options</b>	<ul style="list-style-type: none"><li>• <code>ip-address</code>—Specify IP address of the host.</li><li>• port <code>port-number</code>—Specify 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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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>Firewall User Authentication Feature Guide for Security Devices</i></li><li>• <i>Application Identification Feature Guide for Security Devices</i></li></ul>

## log-prefix

---

<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 1661</a></li><li>• <i>Junos OS System Log Reference</i></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>• <i>Specifying Log File Size, Number, and Archiving Properties</i></li><li>• <a href="#">syslog on page 1689</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 1664</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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></li></ul>

## no-remote-trace

---

See [tracing](#).

## 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>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## 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 1689</a></li><li>• <i>host</i></li></ul>

## security-log

<b>Syntax</b>	security-log { command <i>binary-file-path</i> ; disable; failover (alternate-media   other-routing-engine); }
<b>Hierarchy Level</b>	[edit system processes]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Specify the security log process.
<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 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>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## security-log-percent-full

<b>Syntax</b>	security-log-percent-full <i>percentage</i> ;
<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>	<i>percentage</i> —Percentage of security log capacity at which a security alarm is raised. <b>Range:</b> 0 through 100 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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>

## severity (Security Log)

---

<b>Syntax</b>	severity (alert   critical   debug   emergency   error   info   notice   warning)
<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> <p><b>Default:</b> debug.</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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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>	<b>size</b> —Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). <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 <b>Range:</b> 64 KB through 1 GB <b>Default:</b> 1 MB for MX Series routers and the QFX Series
<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="#">files on page 1678</a></li> </ul>

## system

<b>Syntax</b>	<code>system { ... }</code>
<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.

## 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 1659</a></li> <li>• <i>Junos OS System Log Reference</i></li> <li>• <a href="#">explicit-priority on page 1673</a></li> <li>• <a href="#">time-format on page 1691</a></li> </ul>

## syslog

```


Syntax  syslog {
        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 Configuration Overview on page 1633</a></li><li>• <a href="#">Junos OS System Log Reference</a></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, but not 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 filename]</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 1663</a></li> <li>• <a href="#">Junos OS System Log Reference</a></li> <li>• <a href="#">structured-data on page 1688</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 <code>/var/log</code>. By default, the name of the file is the name of the process being traced.</li> <li><b>files number</b>—Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed to <b>trace-file.0</b>, then <b>trace-file.1</b>, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten. <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> </ul> </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. <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> </li> </ul>

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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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 1672</a></li><li>• <a href="#">no-remote-trace on page 1682</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 246 on page 1642</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 247 on page 1643</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 1660</a></li> <li>• <a href="#">Junos OS System Logging Facilities and Message Severity Levels on page 1642</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>• <a href="#">Specifying Log File Size, Number, and Archiving Properties</a></li><li>• <a href="#">Junos OS System Log Reference</a></li></ul>

## Administration

---

- [System Log Messages on page 1696](#)
- [Operational Commands on page 1697](#)

### System Log Messages

- [Monitoring System Log Messages with the J-Web Event Viewer on page 1696](#)

#### [Monitoring System Log Messages with the J-Web Event Viewer](#)

---

<b>Purpose</b>	Monitor errors and events that occur on the device.
<b>Action</b>	Select <b>Monitor&gt;Events and Alarms&gt;View Events</b> in the J-Web user interface.  The J-Web View Events page displays the following information about each event: <ul style="list-style-type: none"><li>• <b>Process</b>—System process that generated the error or event.</li><li>• <b>Severity</b>— 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:<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></ul></li></ul>

- 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 1643](#)
- [Understanding Binary Format for Security Logs on page 1645](#)
- [Monitoring Overview on page 1231](#)
- [Monitoring Interfaces on page 1382](#)
- *Junos OS Interfaces Library for Security Devices*

## 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 1707</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear log on page 1699</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 1674](#)
  - [show security log on page 1709](#)
  - *System Log Monitoring and Troubleshooting Guide for Security Devices*

## 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 1712</a></li><li>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></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 1513</a></li> <li><a href="#">monitor stop on page 1515</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor list on page 1703</a>
<b>Output Fields</b>	<a href="#">Table 222 on page 1512</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 252: 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 1512</a></li> <li><a href="#">monitor stop on page 1515</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">monitor start on page 1705</a>
<b>Output Fields</b>	<a href="#">Table 223 on page 1513</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 253: 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 1512</a></li><li>• <a href="#">monitor start on page 1513</a></li></ul>
<b>List of Sample Output</b>	<a href="#">monitor stop on page 1706</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 1707</a> <a href="#">Syntax (TX Matrix Router) on page 1707</a>
<b>Syntax</b>	show log <filename   user <username>>
<b>Syntax (TX Matrix Router)</b>	show log <all-lcc   lcc <i>number</i>   scc> <filename   user <username>>
<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>	List log files, display log file contents, or display information about users who have logged in to the router or switch.
<b>Options</b>	none—List all log files.  <all-lcc   lcc <i>number</i>   scc>—(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 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).  <i>filename</i> —(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.  user <username>—(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.
<b>Required Privilege Level</b>	trace
<b>List of Sample Output</b>	<a href="#">show log on page 1707</a> <a href="#">show log filename on page 1708</a> <a href="#">show log user on page 1708</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 Release 11.2 of Junos OS.
<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 1674</a></li> <li>• <a href="#">clear security log on page 1700</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security log on page 1710</a>

**Output Fields** Table 254 on page 1710 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

**Table 254: 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[
cy[/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[
cy[/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[
cy[/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>• <i>System Log Monitoring and Troubleshooting Guide for Security Devices</i></li> <li>• <a href="#">show security log on page 1709</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security log file on page 1712</a>
<b>Output Fields</b>	<a href="#">Table 255 on page 1712</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 255: 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 20

# SNMP MIBs and Traps Monitoring and Troubleshooting Guide for Security Devices

- Overview on page 1715
- Configuration on page 1812
- Administration on page 1963

## Overview

---

- SNMP on page 1715
- SNMPv3 on page 1782
- SNMP Traps on page 1785
- Routing Instances on page 1796
- Device Management on page 1799
- Remote Operations on page 1801
- Remote Monitoring, Health Monitoring, and Service Quality on page 1804

## SNMP

- Understanding the SNMP Implementation in Junos OS on page 1716
- Standard SNMP MIBs Supported by Junos OS on page 1719
- Juniper Networks Enterprise-Specific MIBs on page 1733
- List of SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways Supported Enterprise-Specific MIBs on page 1740
- List of SRX1400, SRX3400, and SRX3600 Services Gateways Supported Enterprise-Specific MIBs on page 1745
- List of SRX5400, SRX5600 and SRX5800 Services Gateways Supported Enterprise-Specific MIBs on page 1750
- Enterprise-Specific MIBs and Supported Devices on page 1756
- MIB Support Details on page 1766
- SNMP MIB Objects Supported by Junos OS for the Set Operation on page 1775

## 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 1716](#)
- [Junos OS SNMP Agent Features on page 1718](#)

### **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 1716](#)
- [SNMP Traps and Informs on page 1717](#)

### **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 1719](#).

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 1733](#).

### ***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 1785](#).

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 1785](#). For information about system logging severity levels for SNMP traps, see [“System Logging Severity Levels for SNMP Traps” on page 1718](#).

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 1823](#).

### ***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 1786](#) and [“Standard SNMP Version 2 Traps” on page 1789](#). For more information about system logging severity levels for enterprise-specific traps, see *Juniper Networks Enterprise-Specific SNMP Version 1 Traps* and *Juniper Networks Enterprise-Specific SNMP Version 2 Traps*.

### ***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 1782](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### Standard SNMP MIBs Supported by Junos OS

Table 256 on page 1720 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, J, 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 256: Standard MIBs Supported on Devices Running Junos OS

MIB/RFC	Platforms							
	M	T	J	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		
Supported tables and objects:								
<ul style="list-style-type: none"> <li>lldpRemManAddrOID, lldpLocManAddrOID, lldpReinitDelay, lldpNotificationInterval, lldpStatsRxPortFramesDiscardedTotal, lldpStatsRxPortFramesError, lldpStatsRxPortTLVsDiscardedTotal, lldpStatsRxPortTLVsUnrecognizedTotal, lldpStatsRxPortAgeoutsTotal</li> </ul>								
IEEE, 802.3ad, <i>Aggregation of Multiple Link Segments</i>	1	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> <p><b>NOTE:</b> EX Series switches do not support the dot3adAggPortTable and dot3adAggPortStatsTable.</p> <ul style="list-style-type: none"> <li>dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount)</li> </ul> <p><b>NOTE:</b> EX Series switches do not support the dot3adAggPortDebugTable.</p> <ul style="list-style-type: none"> <li>dot3adTablesLastChanged</li> </ul> <p><b>NOTE:</b> Gigabit Ethernet interfaces on J Series Services Routers do not support the 802.3ad MIB.</p>								
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

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						LowEnd	MidRange	High-End
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: <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>	1	1	1	1	1	0	0	1
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)	1	1	1	0	0	0	0	0
RFC 1471, <i>Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol</i> (only <b>pppLink</b> group is supported. The <b>pppLink</b> group consists of the <b>pppLcp 1</b> object and the tables <b>pppLinkStatustable</b> and <b>pppLinkConfigTable</b> ).	1	0	0	1	0	0	0	0

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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 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.)	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)	1	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>sysApplInstallPkgTable</b> , <b>sysApplInstallElmtTable</b> , <b>sysApplElmtRunTable</b> , and <b>sysApplMapTable</b> )	1	1	1	1	1	1	0	1

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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 <code>dsx1FarEndConfigTable</code> , <code>dsx1FarEndCurrentTable</code> , <code>dsx1FarEndIntervalTable</code> , <code>dsx1FarEndTotalTable</code> , and <code>dsx1FracTable</code> )	1	1	1	0	0	1	0	0
RFC 2515, <i>Definitions of Managed Objects for ATM Management</i> (except <code>atmVpCrossConnectTable</code> , <code>atmVcCrossConnectTable</code> , and <code>aal5VccTable</code> )	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
RFC 2572, <i>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</i> (read-only access)  <b>NOTE:</b> RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.	1	1	1	1	1	1	0	1
RFC 2576, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>  <b>NOTE:</b> RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.	1	1	1	1	1	1	0	1
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

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 2662, <i>Definitions of Managed Objects for ADSL Lines</i> (J Series Services Routers. All MIB tables, objects, and traps are applicable for the ADSL ATU-R agent.)	1	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>vrrpStatsPacketLengthErrors</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>								
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>	1	1	1	1	0	0	0	1

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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, ptopoConnIsStatic,</b> <b>ptopoConnLastVerifyTime, 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 2933, <i>Internet Group Management Protocol (IGMP) MIB</i>	1	1	1	1	1	1	0	0
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
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>	1	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

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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.								
RFC 3498, <i>Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures</i> (implemented under the Juniper Networks enterprise branch [jnxExperiment])	1	1	1	0	0	0	0	0



Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 3584 <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>	1	1	1	1	1	0	0	1
RFC 3591 <i>Managed Objects for the Optical Interface Type</i>	1	1	1	0	0	0	0	0
<b>optIfOTMnTable</b> (except <b>optIfOTMnOpticalReach</b> , <b>optIfOTMnInterfaceType</b> , and <b>optIfOTMnOrder</b> ), <b>optIfOChConfigTable</b> (except <b>optIfOChDirectionality</b> and <b>optIfOChCurrentStatus</b> ), <b>optIfOTUkConfigTable</b> (except <b>optIfOTUkTraceIdentifierAccepted</b> , <b>optIfOTUkTIMDetMode</b> , <b>optIfOTUkTIMActEnabled</b> , <b>optIfOTUkTraceIdentifierTransmitted</b> , <b>optIfOTUkDEGThr</b> , <b>optIfOTUkDEGM</b> , <b>optIfOTUkSinkAdaptActive</b> , and <b>optIfOTUkSourceAdaptActive</b> ), and <b>optIfODUkConfigTable</b> (except <b>optIfODUkPositionSeqCurrentSize</b> and <b>optIfODUkTtpPresent</b> )								
RFC 3592, <i>Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type</i>	1	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 <b>etherWisDeviceTable</b> , <b>etherWisSectionCurrentTable</b> , and <b>etherWisFarEndPathCurrentTable</b> )	1	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 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	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) <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:               <ul style="list-style-type: none"> <li><b>mplsTunnelResourceMeanRate</b>,</li> <li><b>mplsTunnelResourceMaxBurstSize</b>,</li> <li><b>mplsTunnelResourceMeanBurstSize</b>,</li> <li><b>mplsTunnelResourceExBurstSize</b>,</li> <li><b>mplsTunnelResourceWeight</b>.</li> </ul> </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>	1	1	1	1	0	0	0	0
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> )	1	1	1	0	0	0	0	0

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 4188, <i>Definitions of Managed Objects for Bridges</i> —Supports 802.1D STP (1998). Supports only the following subtrees and objects:	0	0	0	1	1	0	0	0
<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.								
RFC 4318, <i>Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol</i> —Supports 802.1w and 802.1t extensions for RSTP.	1	1	1	1	1	0	0	0
RFC 4363b, <i>Q-Bridge VLAN MIB</i>	0	0	0	1	1	0	0	0
RFC 4382 <i>MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB</i>	1	1	1	1	1	0	0	0
The Junos OS support for RFC 4382 includes the following scalar objects and tables:								
<ul style="list-style-type: none"> <li><b>mplsL3VpnConfiguredVrfs</b></li> <li><b>mplsL3VpnActiveVrfs</b></li> <li><b>mplsL3VpnConnectedInterfaces</b></li> <li><b>mplsL3VpnNotificationEnable</b></li> <li><b>mplsL3VpnVrfConfMaxPossRts</b></li> <li><b>mplsL3VpnVrfConfRteMxThreshTime</b></li> <li><b>mplsL3VpnI1L3L3RcvThresh</b></li> <li><b>mplsL3VpnVrfTable</b></li> <li><b>mplsL3VpnIfConfTable</b></li> <li><b>mplsL3VpnVrfPerfTable</b></li> <li><b>mplsL3VpnVrfRteTable</b></li> <li><b>mplsVpnVrfRTTable</b></li> </ul>								
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

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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)	1	1	1	1	0	0	0	0
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.)	1	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.	1	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 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
RFC 5643, <i>Management Information Base for OSPFv3</i>	1	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>								
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
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)	1	1	1	1	0	0	0	0

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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 <b>[jnxExperiment]</b> . 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>	1	1	1	1	1	0	0	1
Internet draft draft-ietf-idr-bgp4-mibv2-04.txt, <i>Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version</i> (only <b>jnxBgpM2PrefixInPrefixes</b> , <b>jnxBgpM2PrefixInPrefixesAccepted</b> , and <b>jnxBgpM2PrefixInPrefixesRejected</b> objects)	1	1	1	1	1	0	0	1
Internet draft draft-reeder-snmpv3-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> )	1	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 <b>[jnxExperiment]</b> . 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> .)	1	1	1	1	0	0	0	1

Table 256: Standard MIBs Supported on Devices Running Junos OS (*continued*)

MIB/RFC	Platforms							
	M	T	J	MX	EX	SRX		
						LowEnd	MidRange	High-End
Internet draft draft-ietf-idmr-pim-mib-09.txt, <i>Protocol Independent Multicast (PIM) MIB</i>	1	1	1	1	1	0	0	1
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
NOTE: 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 1733](#)
- [Loading MIB Files to a Network Management System on page 1817](#)

### 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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-atm.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chas-defines.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/reference/mibs/mib-jnx-chas-defines.txt).

For more information, see *Chassis MIBs*.

- Chassis Forwarding MIB—Enables J Series Services Routers to fully support the Junos OS health monitor. 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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis-fwdd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/reference/mibs/mib-jnx-hostresources.txt).

For more information, see *Host Resources MIB*.

- IDP Objects MIB—Provides support for monitoring SNMP IDP queries, requests, responses, and failures. This MIB defines the key monitoring and threshold crossing trap support, IDP database update status and trap support, attack-related monitoring and trap support for SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways. This MIB models IDP attributes specific to the appropriate Juniper Networks implementation. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-idp.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-ipsec-vpn.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipv6.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices, services, and traps. This MIB is currently supported by Junos OS for J Series and 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/junos12.1x46/topics/reference/mibs/mib-jnx-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see

[http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-vpn.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/topics/reference/mibs/mib-jnx-vpn.txt).

For more information, see *VPN MIB*.

#### Related Documentation

- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1756](#)
- [Loading MIB Files to a Network Management System on page 1817](#)

#### 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 J Series and SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for J Series and 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*.

- 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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1X46/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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, **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/junos12.1X46/topics/reference/mibs/mib-jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1X46/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1X46/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1X46/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series

and SRX Series devices. For a downloadable version of this MIB, see

[http://www.juniper.net/techpubs/en\\_US/junos12.1X46/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-js-idp.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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/junos12.1X46/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1X46/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.1X46/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 J Series and SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for J Series and 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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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, **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/junos12.1x46/topics/reference/mibs/mib-jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices only. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices product, services and traps. This MIB is currently supported only by Junos OS for J Series and 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-smi.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-user-aaa.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-auth.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis-alarm.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-atm-cos.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bgpmib2.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-bfd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-chassis.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-jsrpd.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-cfgmgmt.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-dcu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-dns.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/jnx-mac.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-event.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-firewall.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-hostresources.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-if-extensions.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipforward.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-flow-mon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipsec-monitor-asp.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ipv4.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-license.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-lsys-securityprofile.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-nat.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-pfe.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-ping.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-policy.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rpf.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-rmon.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-if-ext.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-screening.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-scu.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-js-spu-monitoring.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-syslog.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-traceroute.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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/junos12.1x46/topics/reference/mibs/mib-jnx-util.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 J Series and SRX Series devices. For a downloadable version of this MIB, see [http://www.juniper.net/techpubs/en\\_US/junos12.1x46/topics/reference/mibs/mib-jnx-js-cert.txt](http://www.juniper.net/techpubs/en_US/junos12.1x46/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 257 on page 1757 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 257: 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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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-jdhcipv6.txt">http://www.juniper.net/techpubs/en_US/junos12.1/topics/reference/mibs/mib-jnx-jdhcipv6.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



Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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	

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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	0
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
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

Table 257: Enterprise-Specific MIBs and Supported Devices (*continued*)

Enterprise-Specific MIB	Platforms							
	M	T	J	MX	EX	SRX		
						Low-End	Mid-Range	High-End
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
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 1733](#)
- [Juniper Networks Enterprise-Specific SNMP Traps on page 1785](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Loading MIB Files to a Network Management System on page 1817](#)

## MIB Support Details

Table 258 on page 1766 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 258: MIB Support for Routing Instances (Juniper Networks MIBs)**

Object	Support Class	Description/Notes
jnxProducts(1)	–	Product Object IDs
jnxServices(2)	–	Services
jnxMibs(3) jnxBoxAnatomy(1)	Class 3	Objects are exposed only for the default logical system.
mpls(2)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
ifJnx(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAlarms(4)	Class 3	Objects are exposed only for the default logical system.
jnxFirewalls(5)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxDCUs(6)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxPingMIB(7)	Class 3	Objects are exposed only for the default logical system.
jnxTraceRouteMIB(8)	Class 3	Objects are exposed only for the default logical system.
jnxATM(10)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxIpv6(11)	Class 4	Data is not segregated by routing instance. All instances are exposed.
jnxIpv4(12)	Class 1	<b>jnxIpv4AddrTable(1).</b> Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.



Table 258: MIB Support for Routing Instances (Juniper Networks MIBs) (*continued*)

Object	Support Class	Description/Notes
jnxRmon(13)	Class 3	jnxRmonAlarmTable(1). Objects are exposed only for the default logical system.
jnxLdp(14)	Class 2	jnxLdpTrapVars(1). All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
jnxCos(15) jnxCosIfqStatsTable(1) jnxCosFcTable(2) jnxCosFcIdTable(3) jnxCosQstatTable(4)	Class 3	Objects are exposed only for the default logical system.
jnxScu(16) jnxScuStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxRpf(17) jnxRpfStatsTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxCfgMgmt(18)	Class 3	Objects are exposed only for the default logical system.
jnxPMon(19) jnxPMonFlowTable(1) jnxPMonErrorTable(2) jnxPMonMemoryTable(3)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxSonet(20) jnxSonetAlarmTable(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxAtmCos(21) jnxCosAtmVcTable(1) jnxCosAtmScTable(2) jnxCosAtmVcQstatsTable(3) jnxCosAtmTrunkTable(4)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
ipSecFlowMonitorMIB(22)	—	—

**Table 258: MIB Support for Routing Instances (Juniper Networks MIBs) (continued)**

Object	Support Class	Description/Notes
jnxMac(23) jnxMacStats(1)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
apsMIB(24)	Class 3	Objects are exposed only for the default logical system.
jnxChassisDefines(25)	Class 3	Objects are exposed only for the default logical system.
jnxVpnMIB(26)	Class 2	All instances within a logical system are exposed. Data will not be segregated down to the routing instance level.
jnxSericesInfoMib(27)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxCollectorMIB(28)	Class 1	Only those logical interfaces (and their parent physical interfaces) that belong to a specific routing instance are exposed.
jnxHistory(29)	—	—
jnxSpMIB(32)	Class 3	Objects are exposed only for the default logical system.

[Table 259 on page 1769](#) 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 259: 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 259: Class 1 MIB Objects (Standard and Juniper MIBs) (*continued*)

Class	MIB	Objects
	<b>rfc3020.mib</b>	<b>mfrMIB</b> <b>mfrBundleTable</b> <b>mfrMibBundleLinkObjects</b> <b>mfrBundleIfIndexMappingTable</b> (and related MIB objects)
	<b>ospf2mib.mib</b>	All objects
	<b>ospf2trap.mib</b>	All objects
	<b>bgpmib.mib</b>	All objects
	<b>rfc2819a.mib</b>	Example: <b>etherStatsTable</b>

Table 259: 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 259: 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 260 on page 1773 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 260: 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 261 on page 1774 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 261: 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 262 on page 1775 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 262: 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 1797](#)
- [Trap Support for Routing Instances on page 1799](#)

### SNMP MIB Objects Supported by Junos OS for the Set Operation

The following table lists the SNMP MIB objects that are supported for the **snmp set** operation by Junos OS.

Object Name	Object Identifier
RFC 1907	
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
snmpEnableAuthenTraps	1.3.6.1.2.1.1.30
RFC 2819a	

Object Name	Object Identifier
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
pingCtlDataFill	1.3.6.1.2.1.80.1.2.1.9

Object Name	Object Identifier
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
traceRouteCtlMaxTtl	1.3.6.1.2.1.81.1.2.1.10

Object Name	Object Identifier
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
<b>Enterprise-Specific PING MIB</b>	
jnxPingCtlIfName	1.3.6.1.4.1.2636.3.7.1.2.1.3
jnxPingCtlRoutingIfIndex	1.3.6.1.4.1.2636.3.7.1.2.1.4
jnxPingCtlRoutingIfName	1.3.6.1.4.1.2636.3.7.1.2.1.5
jnxPingCtlRoutingInstanceName	1.3.6.1.4.1.2636.3.7.1.2.1.6
jnxPingCtlRttThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.7
jnxPingCtlRttStdDevThreshold	1.3.6.1.4.1.2636.3.7.1.2.1.8

Object Name	Object Identifier
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
snmpTargetParamsSecurityLevel	1.3.6.1.6.3.12.1.3.1.4

Object Name	Object Identifier
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
usmUserOwnPrivKeyChange	1.3.6.1.6.3.15.1.2.2.1.10

Object Name	Object Identifier
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
snmpCommunityTransportTag	1.3.6.1.6.3.18.1.1.1.6

Object Name	Object Identifier
snmpCommunityStorageType	1.3.6.1.6.3.18.1.1.7
snmpCommunityStatus	1.3.6.1.6.3.18.1.1.8
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 1719](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Enterprise-Specific MIBs and Supported Devices on page 1756](#)

## SNMPv3

- [SNMPv3 Overview on page 1782](#)
- [Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage on page 1783](#)

### 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 1824](#)
- [Configuring MIB Views on page 1821](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1844](#)
- [Configuring SNMP Informs on page 1823](#)

**Related  
Documentation**

- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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](#)

## SNMP Traps

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1785](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1785](#)
- [Standard SNMP Version 1 Traps on page 1786](#)
- [Standard SNMP Version 2 Traps on page 1789](#)
- [Unsupported Standard SNMP Traps on page 1793](#)

### Juniper Networks Enterprise-Specific SNMP Traps

This topic provides pointers to the enterprise-specific SNMP traps supported by the Junos OS.



**NOTE:** All enterprise-specific SNMP traps supported by the Junos OS can be sent in version 1, 2, and 3 formats.

- [Juniper Networks Enterprise-Specific SNMP Version 1 Traps](#)
- [Juniper Networks Enterprise-Specific SNMP Version 2 Traps](#)
- [Juniper Networks Enterprise-Specific License MIB Notifications](#)

**Related  
Documentation**

- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1785](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1843](#)
- [Managing Traps and Informs on page 1963](#)

### 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 1786](#)

- [Standard SNMP Version 2 Traps on page 1789](#)
- [Unsupported Standard SNMP Traps on page 1793](#)

#### Related Documentation

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1785](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1843](#)
- [Managing Traps and Informs on page 1963](#)

### Standard SNMP Version 1 Traps

Table 263 on page 1786 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 *System Log Monitoring and Troubleshooting Guide for Security Devices*.

**Table 263: 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>							
RFC 2925, <i>Definitions</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.

Table 263: 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>of Managed Objects for Remote Ping, Traceroute, and Lookup Operations</i>	<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 263: 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 263: 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>vrrpTrapNewMaster</b>	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW_MASTER_TRAP	All devices running Junos OS.
	<b>vrrpTrapAuthFailure</b>	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_FAILURE_TRAP	All devices running Junos OS.

**Related Documentation**

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1785](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1785](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1843](#)
- [Managing Traps and Informs on page 1963](#)

**Standard SNMP Version 2 Traps**

Table 264 on page 1789 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 264: 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</i>	<b>coldStart</b>	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_COLD_START	All devices running Junos OS.

Table 264: Standard Supported SNMP Version 2 Traps (*continued*)

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
<i>for Version 2 of the Simple Network Management Protocol (SNMPv2)</i>	<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.
<b>Routing Notifications</b>					
<i>BGP 4 MIB</i>	<b>bgpEstablished</b>	1.3.6.1.2.1.15.7.1	–	–	All devices running Junos OS.



Table 264: Standard Supported SNMP Version 2 Traps (*continued*)

Defined in	Trap Name	snmpTrapOID	System Logging Severity Level	Syslog Tag	Supported On
	<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.

Table 264: 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.

The Junos OS also supports the following standard SNMP version 2 traps:

- [SNMP Version 2 MPLS Traps on page 1792](#)

#### **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.

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.

**Related  
Documentation**

- [Juniper Networks Enterprise-Specific SNMP Traps on page 1785](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1785](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1843](#)
- [Managing Traps and Informs on page 1963](#)

### **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 265 on page 1794](#).

Table 265: 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 265: 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> .
	<b>msdpEstablished</b>	Generated when the Multicast Source Discovery Protocol (MSDP) finite state machine (FSM) enters the <b>Established</b> state.
ospf2trap.mib	<b>msdpBackwardTransition</b>	Generated when the MSDP FSM moves from a higher numbered state to a lower numbered state.
	<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 265: 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 1785](#)
- [Standard SNMP Traps Supported on Devices Running Junos OS on page 1785](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)
- [Standard SNMP MIBs Supported by Junos OS on page 1719](#)

## Routing Instances

- [Identifying a Routing Instance on page 1797](#)
- [Understanding SNMP Support for Routing Instances on page 1797](#)
- [Trap Support for Routing Instances on page 1799](#)

### 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 1797](#)
- [Enabling SNMP Access over Routing Instances on page 1858](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)

### 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.

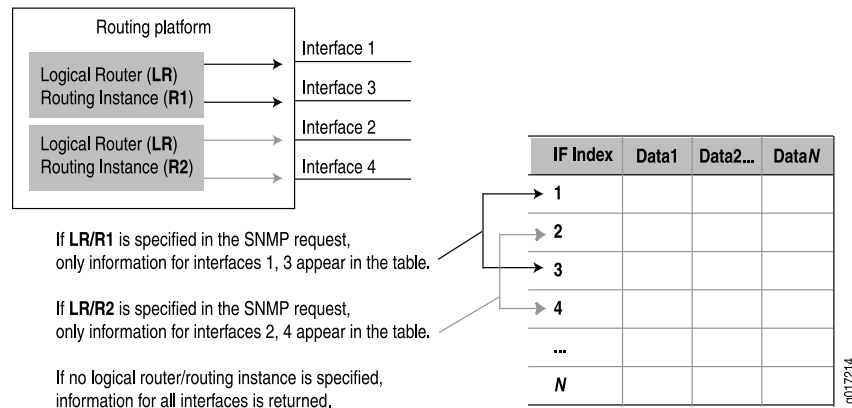
In Junos OS:

- 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 58 on page 1798](#)). Service providers can use this information for their own management needs or export the data for use by their customers.

**Figure 58: 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 1799](#)
- [Identifying a Routing Instance on page 1797](#)
- [Enabling SNMP Access over Routing Instances on page 1858](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1861](#)



### 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 1797](#)
- [MIB Support Details on page 1766](#)

## Device Management

- [Understanding Device Management Functions in Junos OS on page 1799](#)
- [Understanding the Integrated Local Management Interface on page 1801](#)

### 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 266 on page 1800](#).

Table 266: 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 1719 and “<a href="#">Juniper Networks Enterprise-Specific MIBs</a>” on page 1733.</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 1785.</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 1785.</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 1254.</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 1733 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 266: 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 1823 and “Tracing SNMP Activity on a Device Running Junos OS” on page 1968.</li> </ul>

- Related Documentation**
- [Understanding the SNMP Implementation in Junos OS on page 1716](#)
  - [Accounting Options Overview on page 1235](#)

### 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 1799](#)

### Remote Operations

- [SNMP Remote Operations Overview on page 1801](#)

### 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 1802](#)
- [Setting SNMP Views on page 1802](#)
- [Setting Trap Notification for Remote Operations on page 1803](#)
- [Using Variable-Length String Indexes on page 1803](#)
- [Enabling Logging on page 1804](#)

### ***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 1862](#) and **community**.

For more information about the **view** statement, see [“Configuring MIB Views” on page 1821](#), [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 1841](#).

### ***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 1968](#).

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 1966](#)
- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1869](#)

## **Remote Monitoring, Health Monitoring, and Service Quality**

- [Understanding RMON Alarms on page 1804](#)
- [Understanding RMON Events on page 1806](#)
- [Understanding Measurement Points, Key Performance Indicators, and Baseline Values on page 1807](#)
- [Understanding RMON for Monitoring Service Quality on page 1808](#)

### **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 1805
- [jnxRmonAlarmTable](#) on page 1805

### ***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 1806](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)

---

### 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 1806](#)

#### **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 1804](#)
- [Configuring an Event Entry and Its Attributes on page 1874](#)



## 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 1807](#)
- [Basic Key Performance Indicators on page 1808](#)
- [Setting Baselines on page 1808](#)

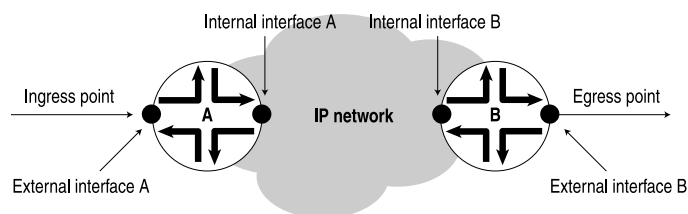
### Measurement Points

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 59 on page 1807](#).

- 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 59: Network Entry Points**



9017042



**NOTE:** [Figure 59 on page 1807](#) 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 1808](#)

---

### **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*.

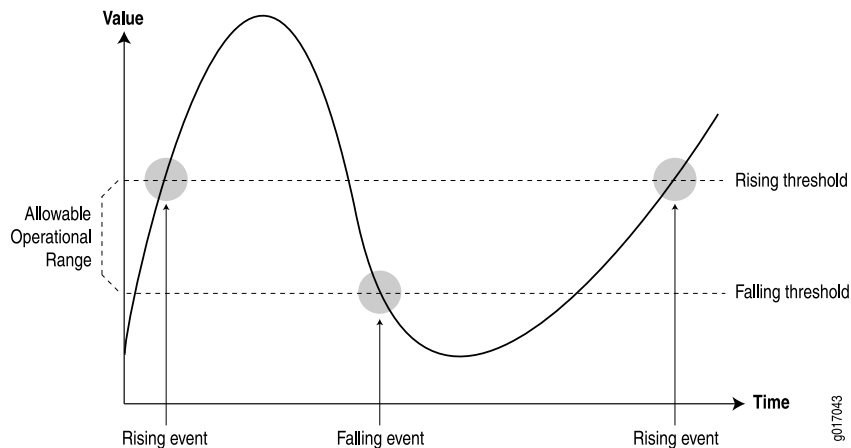
This topic includes the following sections:

- [Setting Thresholds on page 1809](#)
- [RMON Command-Line Interface on page 1810](#)
- [RMON Event Table on page 1810](#)
- [RMON Alarm Table on page 1811](#)
- [Troubleshooting RMON on page 1811](#)

### 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 60 on page 1809](#).)

**Figure 60: 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 267 on page 1810](#).) 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 267: 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

Table 267: RMON Event Table (*continued*)

Field	Description
<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 268 on page 1811](#).

Table 268: 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 269 on page 1811](#) to the RFC 2819 **alarmTable**.

Table 269: jnxRmon Alarm Extensions

Field	Description
<b>jnxRmonAlarmGetFailCnt</b>	Number of times the internal <b>Get</b> request for the variable failed

Table 269: jnxRmon Alarm Extensions (*continued*)

Field	Description
<code>jnxRmonAlarmGetFailTime</code>	Value of <code>sysUpTime</code> when the last failure occurred
<code>jnxRmonAlarmGetFailReason</code>	Reason why the <code>Get</code> request failed
<code>jnxRmonAlarmGetOkTime</code>	Value of <code>sysUpTime</code> when the variable moved out of failure state
<code>jnxRmonAlarmState</code>	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 1807](#)

## Configuration

- [SNMP on page 1812](#)
- [SNMPv3 on page 1824](#)
- [SNMP Traps on page 1836](#)
- [Access Privileges on page 1852](#)
- [Routing Instances on page 1858](#)
- [Community Strings on page 1861](#)
- [Inform Notifications on page 1867](#)
- [Remote Operations on page 1869](#)
- [Remote Monitoring, Health Monitoring, and Service Quality on page 1869](#)
- [Configuration Statements on page 1879](#)

## SNMP

- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1815](#)
- [Configuring the System Description on a Device Running Junos OS on page 1815](#)
- [Configuring the System Location for a Device Running Junos OS on page 1816](#)
- [Configuring the System Name on page 1816](#)
- [Configuring the Commit Delay Timer on page 1817](#)
- [Loading MIB Files to a Network Management System on page 1817](#)
- [Filtering Duplicate SNMP Requests on page 1819](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1820](#)
- [Example: Configuring Secured Access List Checking on page 1820](#)

- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1820](#)
- [Configuring MIB Views on page 1821](#)
- [Example: Ping Proxy MIB on page 1822](#)
- [Configuring the Local Engine ID on page 1823](#)
- [Configuring SNMP Informs on page 1823](#)

### 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 1716](#)
  - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
  - [Complete SNMPv3 Configuration Statements on page 1885](#)

---

### 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 1813](#)
  - [Configuring the System Location for a Device Running Junos OS on page 1816](#)
  - [Configuring the System Description on a Device Running Junos OS on page 1815](#)
  - [Configuring the System Name on page 1816](#)
  - [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

---

### 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 1813](#)
  - [Configuring the System Contact on a Device Running Junos OS on page 1815](#)
  - [Configuring the System Location for a Device Running Junos OS on page 1816](#)
  - [Configuring the System Name on page 1816](#)

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

---

### 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 1813](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1815](#)
- [Configuring the System Description on a Device Running Junos OS on page 1815](#)
- [Configuring the System Name on page 1816](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

---

### 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 1813](#)
- [Configuring the System Contact on a Device Running Junos OS on page 1815](#)
- [Configuring the System Location for a Device Running Junos OS on page 1816](#)
- [Configuring the System Description on a Device Running Junos OS on page 1815](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1719](#)
- [Juniper Networks Enterprise-Specific MIBs on page 1733](#)

### 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 1813](#)
- [Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 1820](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1820](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Example: Configuring Secured Access List Checking on page 1820](#)

### Example: Configuring Secured Access List Checking

---

Grant SNMP access privileges only to 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 1820](#)
- [Filtering Interface Information Out of SNMP Get and GetNext Output on page 1820](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1820](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Example: Ping Proxy MIB on page 1822](#)
- [view \(Configuring a MIB View\) on page 1962](#)
- [oid on page 1921](#)

---

### 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 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Configuring MIB Views on page 1821](#)
- [view \(Configuring a MIB View\) on page 1962](#)
- [oid on page 1921](#)



## 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 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: SNMPv3 Configuration on page 1825](#)

## Configuring SNMP Informs

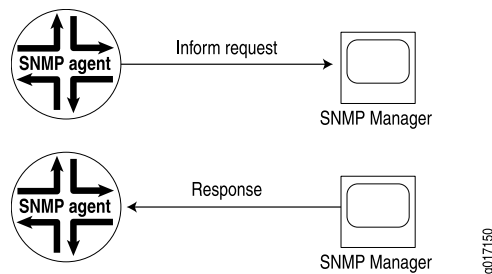
Junos OS supports two types of notifications: traps and informs. With traps, the receiver does not send any acknowledgment when it receives a trap. Therefore, the sender cannot determine if the trap was received. A trap may be lost because a problem occurred during transmission. To increase reliability, 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 61 on page 1824](#)). 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 61: Inform Request and Response**



#### Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1844](#)
- [Configuring the Remote Engine and Remote User on page 1966](#)
- [Configuring the Inform Notification Type and Target Address on page 1867](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## SNMPv3

- [Creating SNMPv3 Users on page 1824](#)
- [Example: SNMPv3 Configuration on page 1825](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Configuring the SNMPv3 Authentication Type on page 1830](#)
- [Configuring the Encryption Type on page 1831](#)
- [Assigning Security Model and Security Name to a Group on page 1833](#)
- [Example: Security Group Configuration on page 1834](#)
- [Example: Configuring the Tag List on page 1835](#)
- [Example: Creating SNMPv3 Users Configuration on page 1835](#)

### 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 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: Creating SNMPv3 Users Configuration on page 1835](#)
- [Example: SNMPv3 Configuration on page 1825](#)

#### 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 1885](#)
  - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1824](#)
- [Configuring MIB Views on page 1821](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1844](#)
- [Configuring SNMP Informs on page 1823](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Example: SNMPv3 Configuration on page 1825](#)

## 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 1830](#)
- [Configuring SHA Authentication on page 1830](#)
- [Configuring No Authentication on page 1831](#)

### 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 1831](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Configuring the Access Privileges Granted to a Group on page 1854](#)
- [Assigning Security Model and Security Name to a Group on page 1833](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1831](#)
- [Configuring the Data Encryption Algorithm on page 1832](#)
- [Configuring Triple DES on page 1832](#)
- [Configuring No Encryption on page 1832](#)

#### 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 1830](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)

- [Configuring the Access Privileges Granted to a Group on page 1854](#)
- [Assigning Security Model and Security Name to a Group on page 1833](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1833](#)
- [Assigning Security Names to Groups on page 1833](#)
- [Configuring the Group on page 1834](#)

#### 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 1824](#). For information about configuring a community string, see [“Configuring the SNMPv3 Community” on page 1864](#).



**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 1853](#).

### 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 1833](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)

- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1844](#)
- [Configuring the Trap Target Address on page 1846](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1885](#)
  - [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## SNMP Traps

- [Configuring SNMP Trap Options on page 1837](#)
- [Configuring the Trap Notification Filter on page 1840](#)
- [Configuring SNMP Trap Groups on page 1841](#)
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS on page 1843](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1844](#)

- [Configuring the SNMPv3 Trap Notification on page 1845](#)
- [Example: Configuring SNMP Trap Groups on page 1846](#)
- [Configuring the Trap Target Address on page 1846](#)
- [Defining and Configuring the Trap Target Parameters on page 1849](#)
- [Example: Configuring SNMPv3 Trap Notification on page 1852](#)

### 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 1841](#).

This topic contains the following sections:

- [Configuring the Source Address for SNMP Traps on page 1837](#)
- [Configuring the Agent Address for SNMP Traps on page 1839](#)
- [Adding snmpTrapEnterprise Object Identifier to Standard SNMP Traps on page 1840](#)

#### 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 1843](#)
- [Configuring SNMP Trap Groups on page 1841](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

---

### ***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 1844](#)
- [Configuring the SNMPv3 Trap Notification on page 1845](#)
- [Configuring the Trap Target Address on page 1846](#)
- [Defining and Configuring the Trap Target Parameters on page 1849](#)
- [Configuring SNMP Informs on page 1823](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1785 and “[Juniper Networks Enterprise-Specific SNMP Traps](#)” on page 1785 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
- **vrrp-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 1843](#)
- [Configuring SNMP Trap Options on page 1837](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Example: Configuring SNMP Trap Groups on page 1846](#)

---

### 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 1837](#)
- [Configuring SNMP Trap Groups on page 1841](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

### 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 1823](#).

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 1845](#)
- [Configuring the Trap Notification Filter on page 1840](#)
- [Configuring the Trap Target Address on page 1846](#)
- [Defining and Configuring the Trap Target Parameters on page 1849](#)
- [Configuring SNMP Informs on page 1823](#)
- [Configuring the Remote Engine and Remote User on page 1966](#)
- [Configuring the Inform Notification Type and Target Address on page 1867](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

### 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 1848.

#### Related Documentation

- [Configuring SNMPv3 Traps on a Device Running Junos OS](#) on page 1844
- [Configuring the Trap Notification Filter](#) on page 1840
- [Configuring the Trap Target Address](#) on page 1846
- [Defining and Configuring the Trap Target Parameters](#) on page 1849
- [Configuring SNMP Informs](#) on page 1823
- [Complete SNMPv3 Configuration Statements](#) on page 1885
- [Minimum SNMPv3 Configuration on a Device Running Junos OS](#) on page 1828
- [Example: Configuring SNMPv3 Trap Notification](#) on page 1852

#### 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 1841
- [Configuring SNMP Trap Options and Groups on a Device Running Junos OS](#) on page 1843
- [Configuring SNMP Trap Options](#) on page 1837

#### 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 1847](#)
- [Configuring the Address Mask on page 1847](#)
- [Configuring the Port on page 1848](#)
- [Configuring the Routing Instance on page 1848](#)
- [Configuring the Trap Target Address on page 1848](#)
- [Applying Target Parameters on page 1849](#)

### **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 1864](#).

### **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 1835](#).

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 1845](#).



**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 1844](#)
- [Configuring the SNMPv3 Trap Notification on page 1845](#)
- [Configuring the Trap Notification Filter on page 1840](#)
- [Defining and Configuring the Trap Target Parameters on page 1849](#)
- [Configuring SNMP Informs on page 1823](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: Configuring the Tag List on page 1835](#)

### 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 1850](#)
- [Configuring the Target Parameters on page 1850](#)

#### ***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 1840](#).

#### ***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 1850](#)
- [Configuring the Security Model on page 1851](#)
- [Configuring the Security Level on page 1851](#)
- [Configuring the Security Name on page 1851](#)

#### ***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 1844](#)
- [Configuring the SNMPv3 Trap Notification on page 1845](#)
- [Configuring the Trap Notification Filter on page 1840](#)
- [Configuring the Trap Target Address on page 1846](#)
- [Configuring SNMP Informs on page 1823](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

#### 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 1844](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## Access Privileges

- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Configuring the Access Privileges Granted to a Group on page 1854](#)
- [Example: Access Privilege Configuration on page 1857](#)

## 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 1821](#).

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 1830](#)
- [Configuring the Access Privileges Granted to a Group on page 1854](#)
- [Assigning Security Model and Security Name to a Group on page 1833](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

---

### Configuring the Access Privileges Granted to a Group

This topic includes the following sections:

- [Configuring the Group on page 1854](#)
- [Configuring the Security Model on page 1854](#)
- [Configuring the Security Level on page 1855](#)
- [Associating MIB Views with an SNMP User Group on page 1855](#)

#### *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 1821](#).

This section describes the following topics related to this configuration:

- [Configuring the Notify View on page 1856](#)
- [Configuring the Read View on page 1856](#)
- [Configuring the Write View on page 1856](#)

#### **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 1830](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Assigning Security Model and Security Name to a Group on page 1833](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)

- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: Access Privilege Configuration on page 1857](#)

### 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 1854](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)

- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## Routing Instances

- [Enabling SNMP Access over Routing Instances on page 1858](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1859](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1861](#)

### 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 1797](#)
- [Identifying a Routing Instance on page 1797](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1861](#)

### 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 1797](#)
- [Identifying a Routing Instance on page 1797](#)
- [Enabling SNMP Access over Routing Instances on page 1858](#)
- [Configuring Access Lists for SNMP Access over Routing Instances on page 1861](#)
- [Example: Configuring Interface Settings for a Routing Instance on page 1859](#)

#### Example: Configuring Interface Settings for a Routing Instance

This example shows an **802.3ad ae0** interface configuration allocated to a routing instance named **INFrtid**:

```

[edit chassis]
aggregated-devices {
  ethernet {
    device-count 5;
  }
}
[edit interfaces ae0]
vlan-tagging;
aggregated-ether-options {
  minimum-links 2;
  link-speed 100m;
}
unit 0 {
  vlan-id 100;
  family inet {
    address 10.1.0.1/24;
  }
}
[edit interfaces fe-1/1/0]
fastether-options {

```

```

    802.3ad ae0;
}
[edit interfaces fe-1/1/1]
fastether-options {
    802.3ad ae0;
}
[edit routing-instances]
INFrt {
    instance-type virtual-router;
    interface fe-1/1/0.0;
    interface fe-1/1/1.0;
    interface fe-1/1/5.0;
    interface ae0.0;
    protocols {
        ospf {
            area 0.0.0.0 {
                interface all;
            }
        }
    }
}
}

```

The following **snmpwalk** command shows how to retrieve SNMP-related information from **router1** and the 802.3ae bundle interface belonging to routing instance **INFrt** with the SNMP community **public**:

```

router# snmpwalk -Os router1 INFrt@public dot3adAggTable
dot3adAggMACAddress.59 = 0:90:69:92:93:f0
dot3adAggMACAddress.65 = 0:90:69:92:93:f0
dot3adAggActorSystemPriority.59 = 0
dot3adAggActorSystemPriority.65 = 0
dot3adAggActorSystemID.59 = 0:0:0:0:0:0
dot3adAggActorSystemID.65 = 0:0:0:0:0:0
dot3adAggAggregateOrIndividual.59 = true(1)
dot3adAggAggregateOrIndividual.65 = true(1)
dot3adAggActorAdminKey.59 = 0
dot3adAggActorAdminKey.65 = 0
dot3adAggActorOperKey.59 = 0
dot3adAggActorOperKey.65 = 0
dot3adAggPartnerSystemID.59 = 0:0:0:0:0:0
dot3adAggPartnerSystemID.65 = 0:0:0:0:0:0
dot3adAggPartnerSystemPriority.59 = 0
dot3adAggPartnerSystemPriority.65 = 0
dot3adAggPartnerOperKey.59 = 0
dot3adAggPartnerOperKey.65 = 0
dot3adAggCollectorMaxDelay.59 = 0
dot3adAggCollectorMaxDelay.65 = 0

```

**Related  
Documentation**

- [Understanding SNMP Support for Routing Instances on page 1797](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)

### 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 1797](#)
- [Enabling SNMP Access over Routing Instances on page 1858](#)
- [Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858](#)

### Community Strings

- [Configuring the SNMP Community String on page 1862](#)
- [Examples: Configuring the SNMP Community String on page 1862](#)
- [Adding a Group of Clients to an SNMP Community on page 1863](#)
- [Configuring the SNMPv3 Community on page 1864](#)
- [Example: SNMPv3 Community Configuration on page 1866](#)

## 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 1821.

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 1863](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Examples: Configuring the SNMP Community String on page 1862](#)

## 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 1862](#)

### 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.

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 on page 1896](#)
  - [client-list-name on page 1896](#)

### 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;
security-name security-name;
tag tag-name;
```

This section includes the following topics:

- [Configuring the Community Name on page 1865](#)
- [Configuring the Security Names on page 1866](#)
- [Configuring the Tag on page 1866](#)

### 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 Security Names

To assign a community string to a security name, include the **security-name** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
security-name security-name;
```

**security-name** is used when access control is set up. The **security-to-group** configuration at the **[edit snmp v3 vacm]** hierarchy level identifies the group.



**NOTE:** This security name must match the security name configured at the **[edit snmp v3 target-parameters target-parameters-name parameters]** hierarchy level when you configure traps.

### Configuring the Tag

To configure the tag, include the **tag** statement at the **[edit snmp v3 snmp-community community-index]** hierarchy level:

```
[edit snmp v3 snmp-community community-index]
tag tag-name;
```

**tag-name** identifies the address of managers that are allowed to use a community string.

#### Related Documentation

- [Creating SNMPv3 Users on page 1824](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: SNMPv3 Community Configuration on page 1866](#)

### 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 1864](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)

- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## Inform Notifications

- [Configuring the Inform Notification Type and Target Address on page 1867](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1868](#)

### 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 1848](#).

**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-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 1844](#)
- [Configuring SNMP Informs on page 1823](#)
- [Configuring the Remote Engine and Remote User on page 1966](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: Configuring the Inform Notification Type and Target Address on page 1868](#)

---

#### 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 1867](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## Remote Operations

- [Using the Traceroute MIB for Remote Monitoring Devices Running Junos OS on page 1869](#)

### 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 1801](#)

## Remote Monitoring, Health Monitoring, and Service Quality

- [Understanding RMON Alarms and Events Configuration on page 1869](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)
- [Configuring an Event Entry and Its Attributes on page 1874](#)
- [Example: Configuring an RMON Alarm and Event Entry on page 1875](#)
- [Configuring Health Monitoring on Devices Running Junos OS on page 1875](#)
- [Example: Configuring Health Monitoring on page 1878](#)

### 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 1804](#)
- [Understanding RMON Events on page 1806](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)
- [Configuring an Event Entry and Its Attributes on page 1874](#)

---

**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 1871](#)
- [Configuring the Description on page 1871](#)
- [Configuring the Falling Event Index or Rising Event Index on page 1871](#)
- [Configuring the Falling Threshold or Rising Threshold on page 1871](#)
- [Configuring the Interval on page 1872](#)
- [Configuring the Falling Threshold Interval on page 1872](#)
- [Configuring the Request Type on page 1873](#)
- [Configuring the Sample Type on page 1873](#)
- [Configuring the Startup Alarm on page 1873](#)
- [Configuring the System Log Tag on page 1874](#)
- [Configuring the Variable on page 1874](#)



### 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 1869](#)
- [Understanding RMON Alarms on page 1804](#)
- [Understanding RMON Events on page 1806](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)
- [Example: Configuring an RMON Alarm and Event Entry on page 1875](#)

---

### 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 1869](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)
- [Configuring an Event Entry and Its Attributes on page 1874](#)

---

### 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 1876](#)
- [Minimum Health Monitoring Configuration on page 1877](#)
- [Configuring the Falling Threshold or Rising Threshold on page 1877](#)
- [Configuring the Interval on page 1878](#)
- [Log Entries and Traps on page 1878](#)

### **Monitored Objects**

When you configure the health monitor, monitoring information for certain object instances is available, as shown in [Table 270 on page 1876](#).

**Table 270: 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> .

Table 270: Monitored Object Instances (*continued*)

Object	Description
<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>sysApplElmtRunCPU</code>	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.
<code>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 1869](#)
- [Configuring an Alarm Entry and Its Attributes on page 1870](#)
- [Configuring an Event Entry and Its Attributes on page 1874](#)
- [Example: Configuring Health Monitoring on page 1878](#)
- [Understanding Device Management Functions in Junos OS on page 1799](#)

---

### **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 1875](#)

## Configuration Statements

- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [access-list on page 1887](#)
- [address on page 1888](#)
- [address-mask on page 1888](#)
- [agent-address on page 1889](#)
- [alarm on page 1890](#)
- [authentication-md5 on page 1891](#)
- [authentication-none on page 1892](#)
- [authentication-password on page 1893](#)
- [authentication-sha on page 1894](#)
- [authorization on page 1895](#)
- [categories on page 1895](#)
- [client-list on page 1896](#)
- [client-list-name on page 1896](#)
- [clients on page 1897](#)
- [commit-delay on page 1897](#)
- [community on page 1898](#)
- [community on page 1899](#)
- [community-name on page 1900](#)
- [contact on page 1901](#)
- [description on page 1901](#)
- [description on page 1902](#)
- [destination-port on page 1902](#)
- [engine-id on page 1903](#)
- [enterprise-oid on page 1904](#)
- [event on page 1904](#)

- [falling-event-index](#) on page 1905
- [falling-threshold](#) on page 1906
- [falling-threshold](#) on page 1907
- [falling-threshold-interval](#) on page 1908
- [filter-duplicates](#) on page 1908
- [filter-interfaces](#) on page 1909
- [group \(Configuring Group Name\)](#) on page 1910
- [group \(Defining Access Privileges for an SNMPv3 Group\)](#) on page 1911
- [health-monitor](#) on page 1911
- [interface](#) on page 1912
- [interval](#) on page 1912
- [interval](#) on page 1913
- [local-engine](#) on page 1914
- [location](#) on page 1915
- [logical-system](#) on page 1916
- [logical-system-trap-filter](#) on page 1917
- [message-processing-model](#) on page 1917
- [name](#) on page 1918
- [nonvolatile](#) on page 1918
- [notify](#) on page 1919
- [notify-filter \(Applying to the Management Target\)](#) on page 1919
- [notify-filter \(Configuring the Profile Name\)](#) on page 1920
- [notify-view](#) on page 1920
- [oid](#) on page 1921
- [oid](#) on page 1921
- [parameters](#) on page 1922
- [port](#) on page 1922
- [privacy-3des](#) on page 1923
- [privacy-aes128](#) on page 1924
- [privacy-des](#) on page 1925
- [privacy-none](#) on page 1925
- [privacy-password](#) on page 1926
- [read-view](#) on page 1927
- [remote-engine](#) on page 1928
- [request-type](#) on page 1929
- [retry-count](#) on page 1929
- [rising-event-index](#) on page 1930

- [rising-threshold on page 1930](#)
- [rising-threshold on page 1931](#)
- [rmon on page 1931](#)
- [routing-engine \(SNMP Resource Level\) on page 1932](#)
- [routing-engine \(SNMP Global Level\) on page 1933](#)
- [routing-instance on page 1934](#)
- [routing-instance on page 1935](#)
- [routing-instance-access on page 1935](#)
- [sample-type on page 1936](#)
- [security-level \(Defining Access Privileges\) on page 1937](#)
- [security-level \(Generating SNMP Notifications\) on page 1938](#)
- [security-model \(Access Privileges\) on page 1939](#)
- [security-model \(Group\) on page 1940](#)
- [security-model \(SNMP Notifications\) on page 1940](#)
- [security-name \(Community String\) on page 1941](#)
- [security-name \(Security Group\) on page 1941](#)
- [security-name \(SNMP Notifications\) on page 1942](#)
- [security-to-group on page 1943](#)
- [snmp on page 1943](#)
- [source-address on page 1944](#)
- [snmp-community on page 1944](#)
- [startup-alarm on page 1945](#)
- [syslog-subtag on page 1945](#)
- [tag on page 1946](#)
- [tag-list on page 1946](#)
- [target-address on page 1947](#)
- [target-parameters on page 1948](#)
- [targets on page 1949](#)
- [timeout on page 1949](#)
- [traceoptions on page 1950](#)
- [trap-group on page 1952](#)
- [trap-options on page 1953](#)
- [type on page 1953](#)
- [type on page 1954](#)
- [user on page 1954](#)
- [usm on page 1955](#)
- [v3 on page 1957](#)

- [vacm](#) on page 1959
- [variable](#) on page 1960
- [version](#) on page 1960
- [view \(Associating a MIB View with a Community\)](#) on page 1961
- [view \(Configuring a MIB View\)](#) on page 1962
- [write-view](#) on page 1963

---

### 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 1716](#)
- [Configuring SNMP on a Device Running Junos OS on page 1813](#)

### 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 1824](#)
- [Configuring MIB Views on page 1821](#)
- [Defining Access Privileges for an SNMP Group on page 1853](#)
- [Configuring SNMPv3 Traps on a Device Running Junos OS on page 1844](#)
- [Configuring SNMP Informs on page 1823](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## access-list

**Syntax**

```
[edit snmp]
  routing-instance-access {
    access-list {
      routing-instance;
      routing-instance restrict;
    }
  }
```

**Hierarchy Level** [edit snmp routing-instance-access]

**Release Information** Statement introduced in Junos OS Release 8.4.

**Description** 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 **restrict** keyword.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**Related Documentation**

- [routing-instance-access on page 1935](#)

## address

---

<b>Syntax</b>	<code>address <i>address</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>	Specify the SNMP target address.
<b>Options</b>	<b><i>address</i></b> —IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1847</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 1847</a></li></ul>

## agent-address

---

<b>Syntax</b>	agent-address outgoing-interface;
<b>Hierarchy Level</b>	[edit snmp trap-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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 1839</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>	<p><i>index</i>—Identifies this alarm entry as an integer.</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 an Alarm Entry and Its Attributes on page 1870</a></li><li>• <a href="#">event on page 1904</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 1830</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 1831</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 1830</a></li> <li>• <a href="#">Configuring SHA Authentication on page 1830</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 1830</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><i>authorization</i>—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> <code>read-only</code></p>
<b>Required Privilege Level</b>	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—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 1862</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>	<i>category</i> —Name of a trap type: <b>authentication</b> , <b>chassis</b> , <b>configuration</b> , <b>link</b> , <b>remote-operations</b> , <b>rmon-alarm</b> , <b>routing</b> , <b>sonet-alarms</b> , <b>startup</b> , or <b>vrp-events</b> .
<b>Required Privilege Level</b>	<p><code>snmp</code>—To view this statement in the configuration.</p> <p><code>snmp-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring SNMP Trap Groups on page 1841</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 1863</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 1863</a></li></ul>

## clients

<b>Syntax</b>	clients { <i>address</i> <restrict>; }
<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 1862</a></li> </ul>

## commit-delay

<b>Syntax</b>	commit-delay <i>seconds</i> ;
<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 1817</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 1862</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><i>community-name</i></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 1874</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 1864</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 1815</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 1815</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>	<b><i>description</i></b> —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 1871</a></li><li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1874</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>	<b><i>port-number</i></b> —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 1841</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 1823</a></li> </ul>

## enterprise-oid

---

Syntax	enterprise-oid;
Hierarchy Level	[edit snmp <a href="#">trap-options</a> ]
Release Information	Statement introduced in Junos OS Release 10.0
Description	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.
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"><li>• <a href="#">Configuring SNMP Trap Options on page 1837</a></li></ul>

## event

---

Syntax	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> ; }
Hierarchy Level	[edit snmp <a href="#">rmon</a> ]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure RMON event entries.
Options	<i>index</i> —Identifier for a specific event entry.  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	<ul style="list-style-type: none"><li>• <a href="#">Configuring an Event Entry and Its Attributes on page 1874</a></li><li>• <a href="#">alarm on page 1890</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>	<b><i>index</i></b> —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>	<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 Falling Event Index or Rising Event Index on page 1871</a></li><li>• <a href="#">rising-event-index on page 1930</a></li></ul>

## falling-threshold

---

<b>Syntax</b>	<code>falling-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 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 1877</a></li><li>• <a href="#">rising-threshold on page 1931</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 1871</a></li><li>• <a href="#">rising-threshold on page 1930</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 1872</a></li><li>• <a href="#">interval on page 1912</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 1819</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>	<p>Statement introduced in Junos OS Release 9.4.</p> <p>Statement introduced in Junos OS Release 9.4 for EX Series Switches.</p>
<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 1820</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 1854](#)



## group (Defining Access Privileges for an SNMPv3 Group)

---

<b>Syntax</b>	<code>group <i>group-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 vacm security-to-group security-model (usm   v1   v2c)     <i>security-name security-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 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 1834</a></li> </ul>

## health-monitor

---

<b>Syntax</b>	<pre>health-monitor {     <i>falling-threshold percentage</i>;     <i>interval seconds</i>;     <i>rising-threshold percentage</i>; }</pre>
<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>	<p>Configure health monitoring.</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 Health Monitoring on Devices Running Junos OS on page 1875</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 1820</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 1872</a></li></ul>

## interval

---

<b>Syntax</b>	interval <i>seconds</i> ;
<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><i>seconds</i></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 1878</a></li></ul>

## local-engine


<b>Syntax</b>	<pre> 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;     }   } } </pre>
<b>Hierarchy Level</b>	[edit snmp v3 <a href="#">usm</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>	<p>Configure local engine information for the user-based security model (USM).</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="#">Creating SNMPv3 Users on page 1824</a></li> </ul>

## 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 1816</a></li></ul>

## logical-system

<b>Syntax</b>	<pre>logical-system <i>logical-system-name</i> {     <i>routing-instance routing-instance-name</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[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>]</pre>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
<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 1858</a></li> <li>• <a href="#">Configuring the Trap Target Address on page 1846</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 1799</a></li> </ul>

## message-processing-model

---

<b>Syntax</b>	message-processing-model (v1   v2c   v3);
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameter-name</i> parameters]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	v1—SNMPv1 message process model.  v2c—SNMPv2c message process model.  v3—SNMPv3 message process 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 Message Processing Model on page 1850</a></li> </ul>

## name

---

<b>Syntax</b>	<code>name <i>name</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>	Set the system name from the command-line interface.
<b>Options</b>	<i>name</i> —System name override.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 Name on page 1816</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 1817</a></li><li>• <a href="#">commit-delay on page 1897</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 1867</a></li> <li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1845</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 1850</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 1840</a></li><li>• <a href="#">oid on page 1921</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 1821</a></li><li>• <a href="#">Configuring the Notify View on page 1856</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>	<p><b>exclude</b>—Exclude the subtree of MIB objects represented by the specified OID.</p> <p><b>include</b>—Include the subtree of MIB objects represented by the specified OID.</p> <p><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.</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 MIB Views on page 1821</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>	<p><b>exclude</b>—Exclude the subtree of MIB objects represented by the specified OID.</p> <p><b>include</b>—Include the subtree of MIB objects represented by the specified OID.</p> <p><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.</p>
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Trap Notification Filter on page 1840</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>	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 a set of target parameters for message processing and security.  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 and Configuring the Trap Target Parameters on page 1849</a></li></ul>

## port

---

<b>Syntax</b>	<pre>port port-number;</pre>
<b>Hierarchy Level</b>	[edit snmp v3 target-address <i>target-address-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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 a UDP port number for an SNMP target.
<b>Default</b>	If you omit this statement, the default port is 162.
<b>Options</b>	<i>port-number</i> —Port number for the SNMP target.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring the Port on page 1848</a></li></ul>

## privacy-3des

---

<b>Syntax</b>	<pre>privacy-3des {     <b>privacy-password</b> <i>privacy-password</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[edit snmp v3 usm local-engine user <i>username</i>], [edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i>]</pre>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	<p>Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.</p>
<b>Options</b>	<p><b>privacy-password</b> <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"> <li>• The password must be at least eight characters long.</li> <li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li> </ul>
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Encryption Type on page 1831</a></li> </ul>

## privacy-aes128

---

<b>Syntax</b>	<pre>privacy-aes128 {     <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 Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.
<b>Options</b>	<p><b>privacy-password</b> <i>privacy-password</i>—Password that a user enters. The password is then converted into a key that is used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a router or switch:</p> <ul style="list-style-type: none"><li>• The password must be at least eight characters long.</li><li>• The password can include alphabetic, numeric, and special characters, but it cannot include control characters.</li></ul>
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1831</a></li></ul>

## privacy-des

<b>Syntax</b>	<code>privacy-des {     <b>privacy-password</b> <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>	<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 1831</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 1831</a></li> </ul>

## privacy-password

---

<b>Syntax</b>	<code>privacy-password <i>privacy-password</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 usm local-engine user <i>username</i> privacy-3des],</code> <code>[edit snmp v3 usm local-engine user <i>username</i> privacy-aes128],</code> <code>[edit snmp v3 usm local-engine user <i>username</i> privacy-des],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-3des],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-aes128],</code> <code>[edit snmp v3 usm remote-engine <i>engine-id</i> user <i>username</i> privacy-des]</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 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>	<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 Encryption Type on page 1831</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 1856</a></li><li>• <a href="#">Configuring MIB Views on page 1821</a></li></ul>

## remote-engine

<b>Syntax</b>	<pre> remote-engine <i>engine-id</i> {   user <i>username</i> {     authentication-md5 {       authentication-password <i>authentication-password</i>;     }     authentication-none;     authentication-sha {       authentication-password <i>authentication-password</i>;     }     privacy-aes128 {       privacy-password <i>privacy-password</i>;     }     privacy-des {       privacy-password <i>privacy-password</i>;     }     privacy-3des {       privacy-password <i>privacy-password</i>;     }     privacy-none {       privacy-password <i>privacy-password</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit snmp v3 usm]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p>
<b>Description</b>	Configure the remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.
<b>Options</b>	<p><b><i>engine-id</i></b>—Engine identifier. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Configuring the Remote Engine and Remote User on page 1966</a></li> </ul>

## request-type

<b>Syntax</b>	<code>request-type (get-next-request   get-request   walk-request);</code>
<b>Hierarchy Level</b>	[edit snmp rmon <a href="#">alarm index</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3. 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>	<p><b>get-next-request</b>—Performs an SNMP get next request.</p> <p><b>get-request</b>—Performs an SNMP get request.</p> <p><b>walk-request</b>—Performs an SNMP walk request.</p> <p><b>Default:</b> walk-request</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 Request Type on page 1873</a></li> <li>• <a href="#">variable on page 1960</a></li> </ul>

## retry-count

<b>Syntax</b>	<code>retry-count <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit snmp v3 <a href="#">target-address target-address-name</a> ]
<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>	<p><b>number</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.</p> <p><b>Default:</b> 3 times</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 Informs on page 1823</a></li> <li>• <a href="#">timeout on page 1949</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>	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 1871</a></li><li>• <a href="#">falling-event-index on page 1905</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>	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 1871</a></li><li>• <a href="#">falling-threshold on page 1907</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>	<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="#">falling-threshold on page 1906</a></li> <li>• <a href="#">Configuring the Falling Threshold or Rising Threshold on page 1877</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>	<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 an Alarm Entry and Its Attributes on page 1870</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>	<p>Specify a routing instance for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use this routing instance.</p> <p>If the routing instance is defined within a logical system, include the <b>logical-system</b> <i>logical-system-name</i> statement at the <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.</p>
<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 1841</a></li><li>• <a href="#">Configuring the Source Address for SNMP Traps on page 1837</a></li><li>• <a href="#">Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community on page 1858</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>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Trap Target Address on page 1846</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>	<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="#">Enabling SNMP Access over Routing Instances on page 1858</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 1873</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>	<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>	Define the security level used for access privileges.
<b>Default</b>	none
<b>Options</b>	<p><b>authentication</b>—Provide authentication but no encryption.</p> <p><b>none</b>—No authentication and no encryption.</p> <p><b>privacy</b>—Provide authentication and encryption.</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 Security Level on page 1855</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 1851</a></li></ul>

## security-model (Access Privileges)

---

<b>Syntax</b>	<code>security-model (usm   v1   v2c);</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 vacm access group <i>group-name</i> (default-context-prefix   context-prefix <i>context-prefix</i>)]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	<code>usm</code> —SNMPv3 security model.  <code>v1</code> —SNMPv1 security model.  <code>v2c</code> —SNMPv2c security 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 Security Model on page 1854</a></li> </ul>

## security-model (Group)

---

<b>Syntax</b>	<pre>security-model (usm   v1   v2c) {     security-name security-name {         group group-name;     } }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 vacm <a href="#">security-to-group</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Define a security model for a group.
<b>Options</b>	<b>usm</b> —SNMPv3 security model.  <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 1833</a></li></ul>

## security-model (SNMP Notifications)

---

<b>Syntax</b>	<pre>security-model (usm   v1   v2c);</pre>
<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 model for an SNMPv3 group. The security model is used for SNMP notifications.
<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 1851</a></li></ul>

## security-name (Community String)

Syntax	<code>security-name <i>security-name</i>;</code>
Hierarchy Level	<code>[edit snmp v3 <b>snmp-community</b> <i>community-index</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Associate the community string configured at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level to a security name.
Options	<i>security-name</i> —Name used when performing access control.




**NOTE:** The security name must match the configured security name at the `[edit snmp v3 target-parameters target-parameters-name parameters]` hierarchy level when you configure traps or informs.

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"> <li>• <a href="#">Configuring the Security Names on page 1866</a></li> </ul>

## security-name (Security Group)

Syntax	<code>security-name <i>security-name</i> {     <b>group</b> <i>group-name</i>; }</code>
Hierarchy Level	<code>[edit snmp v3 vacm security-to-group <b>security-model</b> (usm   v1   v2c)]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Associate a group or a community string with a configured security group.
Options	<i>security-name</i> —Username configured at the <code>[edit snmp v3 usm local-engine user <i>username</i>]</code> hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the <code>[edit snmp v3 snmp-community <i>community-index</i>]</code> hierarchy level.
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"> <li>• <a href="#">Assigning Security Names to Groups on page 1833</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 1851</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 1833</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 1813</a></li> </ul>

## source-address

<b>Syntax</b>	<code>source-address <i>address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp trap-options]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. 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>	<p><b><i>address</i></b>—Source address of SNMP traps. You can configure the source address of trap packets two ways: <b>lo0</b> or a valid IPv4 address configured on one of the router interfaces. The value <b>lo0</b> indicates that the source address of all SNMP trap packets is set to the lowest loopback address configured at interface <b>lo0</b>.</p> <p><b>Default:</b> Disabled. (The source address is the address of the outgoing interface.)</p>
<b>Required Privilege Level</b>	<p><b>snmp</b>—To view this statement in the configuration.</p> <p><b>snmp-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Source Address for SNMP Traps on page 1837</a></li> </ul>

## snmp-community

<b>Syntax</b>	<pre>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>; }</pre>
<b>Hierarchy Level</b>	<code>[edit snmp v3]</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 the SNMP community.
<b>Options</b>	<p><b><i>community-index</i></b>—(Optional) String that identifies an SNMP community.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p><b>snmp</b>—To view this statement in the configuration.</p> <p><b>snmp-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the SNMPv3 Community on page 1864</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 1873</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 1874</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>	<i>tag-name</i> —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 1866</a></li><li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1845</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>	<i>tag-list</i> —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 1848</a></li></ul>

## target-address

---

<b>Syntax</b>	<pre>target-address <i>target-address-name</i> {   address <i>address</i>;   address-mask <i>address-mask</i>;   logical-system <i>logical-system</i>;   port <i>port-number</i>;   retry-count <i>number</i>;   routing-instance <i>instance</i>;   tag-list <i>tag-list</i>;   target-parameters <i>target-parameters-name</i>;   timeout <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
<b>Description</b>	Configure the address of an SNMP management application and the parameters to be used in sending notifications.
<b>Options</b>	<p><b><i>target-address-name</i></b>—String that identifies the target address.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring the Trap Target Address on page 1846</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 1849](#)
- [Applying Target Parameters on page 1849](#)

## 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>	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 1841</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>	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 Informs on page 1823</a></li> <li>• <a href="#">retry-count on page 1929</a></li> </ul>

## traceoptions

<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>	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="#">Tracing SNMP Activity on a Device Running Junos OS on page 1968</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 1841</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 1837</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 1823</a></li> <li>• <a href="#">Configuring the SNMPv3 Trap Notification on page 1845</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 1874</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 1824</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 1824</a></li><li>• <a href="#">Configuring the Remote Engine and Remote User on page 1966</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 1828</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 1853</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 1874</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 1841</a></li></ul>


## view (Associating a MIB View with a Community)

---

<b>Syntax</b>	<code>view <i>view-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp community <i>community-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Associate a view with a community. A view represents a group of MIB objects.
<b>Options</b>	<b><i>view-name</i></b> —Name of the view. You must use a view name already configured in the <b>view</b> statement at the <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 1862</a></li></ul>

## view (Configuring a MIB View)

---

Syntax	<pre>view <i>view-name</i> {     <i>oid object-identifier</i> (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 <b>[edit snmp community <i>community-name</i>]</b> hierarchy level.
<div> <b>NOTE:</b> To remove an OID completely, use the <b>delete view all oid oid-number</b> command but omit the <b>include</b> parameter.</div>	
Options	<p><b><i>view-name</i></b>—Name of the view.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	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"><li>• <a href="#">Configuring MIB Views on page 1821</a></li><li>• <a href="#">Associating MIB Views with an SNMP User Group on page 1855</a></li><li>• <a href="#">community on page 1898</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>	<b><i>view-name</i></b> —Name of the view for which the SNMP user group has write permission.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. 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 1821</a></li> <li>• <a href="#">Configuring the Write View on page 1856</a></li> </ul>

## Administration

---

- [SNMP Traps on page 1963](#)
- [Remote Operations on page 1966](#)
- [Tracing Activity on page 1968](#)
- [Ping Tests on page 1972](#)
- [Operational Commands on page 1978](#)

## SNMP Traps

- [Managing Traps and Informs on page 1963](#)

### Managing Traps and Informs

---

The following sections contain a few tips on managing SNMP notifications:

- [Generating Traps Based on SysLog Events on page 1963](#)
- [Filtering Traps Based on the Trap Category on page 1964](#)
- [Filtering Traps Based on the Object Identifier on page 1964](#)

#### **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`, `vrp-events`, `services`, and `otn-alarms` traps:

```
[edit snmp]
trap-group jnpr {
  categories {
    link;
    vrp-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 tg1;
  target-parameters TP_v2c_trap;
}
target-parameters TP_v2c_trap {
  parameters {
    message-processing-model v2c;
    security-model v2c;
    security-level none;
    security-name sn_v2c_trap;
  }
  notify-filter nf1;
}
notify v2c_notify {
  type trap;
  tag tg1;
}
notify-filter nf1 {
  oid .1.3.6.1.4.1.2636.4.5 exclude;
  oid .1 include;
}
snmp-community index1 {
  community-name "$ABC123"; ## SECRET-DATA
  security-name sn_v2c_trap;
  tag tg1;
}
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 Operations

- [Using the Ping MIB for Remote Monitoring Devices Running Junos OS on page 1966](#)
- [Configuring the Remote Engine and Remote User on page 1966](#)
- [Example: Configuring the Remote Engine ID and Remote Users on page 1967](#)

---

### 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 1801](#)
  - [Starting a Ping Test on page 1972](#)
  - [Monitoring a Running Ping Test on page 1973](#)
  - [Gathering Ping Test Results on page 1976](#)
  - [Stopping a Ping Test on page 1977](#)
  - [Interpreting Ping Variables on page 1977](#)

---

### 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 1844](#)
- [Configuring SNMP Informs on page 1823](#)
- [Configuring the Inform Notification Type and Target Address on page 1867](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)
- [Example: Configuring the Remote Engine ID and Remote Users on page 1967](#)

#### 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 {
    authentication-md5 {

```

```
        authentication-key "$ABC123"
    }
    privacy-des {
        privacy-key "$ABC123"
    }
}
}
```

**Related  
Documentation**

- [Configuring the Remote Engine and Remote User on page 1966](#)
- [Complete SNMPv3 Configuration Statements on page 1885](#)
- [Minimum SNMPv3 Configuration on a Device Running Junos OS on page 1828](#)

## Tracing Activity

- [Tracing SNMP Activity on a Device Running Junos OS on page 1968](#)
- [Example: Tracing SNMP Activity on page 1971](#)

### 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 1969](#)
- [Configuring Access to the Log File on page 1969](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 1970](#)
- [Configuring the Trace Operations on page 1970](#)

### **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 271 on page 1970 describes the meaning of the SNMP tracing flags.

**Table 271: 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

Table 271: SNMP Tracing Flags (*continued*)

Flag	Description	Default Setting
<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 1813](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)
- [Example: Tracing SNMP Activity on page 1971](#)

#### 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 1813](#)
- [Tracing SNMP Activity on a Device Running Junos OS on page 1968](#)
- [Configuration Statements at the \[edit snmp\] Hierarchy Level on page 1882](#)

## Ping Tests

- [Starting a Ping Test on page 1972](#)
- [Monitoring a Running Ping Test on page 1973](#)
- [Gathering Ping Test Results on page 1976](#)
- [Stopping a Ping Test on page 1977](#)
- [Interpreting Ping Variables on page 1977](#)

---

### 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 1802](#).

There are two ways to start a ping test:

- [Using Multiple Set Protocol Data Units \(PDUs\) on page 1972](#)
- [Using a Single Set PDU on page 1973](#)

#### ***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 1973
- [pingProbeHistoryTable](#) on page 1975
- [Generating Traps](#) on page 1975

### *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 1975.

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 1841](#) and [“Example: Setting Trap Notification for Remote Operations” on page 1803](#).

### 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 1973](#). For more information about Ping MIB traps, see [“Generating Traps” on page 1975](#).

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 272 on page 1976](#).

**Table 272: Results in `pingProbeHistoryTable`: After the First Ping Test**

<code>pingProbeHistoryIndex</code>	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 273 on page 1977](#).

**Table 273: Results in pingProbeHistoryTable: After the First Probe of the Second Test**

pingProbeHistoryIndex	Probe Result
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
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 274 on page 1977](#).

**Table 274: 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.

## 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 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>	<p><b>none</b>—Display information about all health monitor alarms and logs.</p> <p><b>alarms &lt;detail&gt;</b>—(Optional) Display detailed information about health monitor alarms.</p> <p><b>logs</b>—(Optional) Display information about health monitor logs.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show snmp health-monitor on page 1981</a> <a href="#">show snmp health-monitor alarms detail on page 1982</a> <a href="#">show snmp health-monitor alarms brief on page 1983</a>
<b>Output Fields</b>	Table 275 on page 1979 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 275: 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 275: 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 275: 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: sysAppElmtRunMemory.5.6.1255
Instance Description: Management process
Instance Value: 38284
Instance State: active

Instance Name: sysAppElmtRunMemory.5.6.3816
Instance Description: Management process
Instance Value: 38352
Instance State: active

Instance Name: sysAppElmtRunMemory.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 1979</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show snmp health-monitor routing-engine history on page 1986</a> <a href="#">show snmp health-monitor routing-engine history extensive on page 1987</a> <a href="#">show snmp health-monitor routing-engine history terse on page 1988</a>
<b>Output Fields</b>	<a href="#">Table 276 on page 1985</a> 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 276: 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 276: 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 1985</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show snmp health-monitor routing-engine status on page 1989</a>
<b>Output Fields</b>	Table 277 on page 1989 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 277: 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>
<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 1992</a></p> <p><a href="#">show snmp mib walk (HA) on page 1992</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStats on page 1993</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStatsIPv4 on page 1993</a></p> <p><a href="#">show snmp mib walk jnxJsPolicySystemStatsTotalAllowIPv4Packets on page 1993</a></p>
<b>Output Fields</b>	Table 278 on page 1991 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 278: 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

```



## CHAPTER 21

# IDP Monitoring and Troubleshooting Guide for Security Devices

- [Overview on page 1995](#)
- [Configuration on page 1999](#)
- [Administration on page 2176](#)

## Overview

---

- [IDP Logging on page 1995](#)
- [Packet Capture on page 1997](#)
- [Tuning on page 1998](#)

## IDP Logging

- [Understanding IDP Logging on page 1995](#)
- [Understanding IDP Log Suppression Attributes on page 1996](#)
- [Understanding IDP Log Information Usage on the IC Series UAC Appliance on page 1997](#)

### Understanding IDP Logging

---

The basic Junos OS system logging continues to function after Intrusion Detection and Prevention (IDP) is enabled. An IDP-enabled device continues to record events that occur because of routine operations, such as a user login into the configuration database. It records failure and error conditions, such as failure to access a configuration file. You can configure files to log system messages and also assign attributes, such as severity levels, to messages. In addition to the regular system log messages, IDP generates event logs for attacks.

IDP generates event logs when an event matches an IDP policy rule in which logging is enabled. When you configure a rule for logging, the device creates a log entry for each event that matches that rule. You can use the CLI or J-Web to configure the policy rules to generate event logs.

Because IDP event logs are generated during an attack, log generation happens in bursts, generating a much larger volume of messages during an attack. In comparison to other event messages, the message size is also much larger for attack generated messages.

The log volume and message size are important concerns for log management. To better manage the volume of log messages, IDP supports log suppression.

By configuring log suppression you can suppress multiple instances of the same log occurring from the same or similar sessions over the same period of time. Enabling log suppression ensures that minimal numbers of logs are generated for the same event or attack that occurs multiple times.

**Related  
Documentation**

- *IDP Policies Overview*
- *Understanding Application-Level DDoS Logging*
- [Understanding IDP Log Suppression Attributes on page 1996](#)
- [Understanding Security Packet Capture on page 1998](#)
- [Understanding IDP Log Information Usage on the IC Series UAC Appliance on page 1997](#)
- *IDP Monitoring and Troubleshooting Guide for Security Devices*

---

### Understanding IDP Log Suppression Attributes

Log suppression ensures that minimal numbers of logs are generated for the same event or attack that occurs multiple times. Log suppression is enabled by default. You can configure certain log suppression attributes to suppress logs according to your needs. When configuring log suppression, keep in mind that log suppression can negatively impact sensor performance if you set the reporting interval too high.

You can configure the following log suppression attributes:

- Include destination addresses while performing log suppression—You can choose to combine log records for events with a matching source address. By default, the IDP sensor does not consider destination when matching events for log suppression.
- Number of log occurrences after which log suppression begins—You can specify the number of instances that a specific event must occur before log suppression begins. By default, log suppression begins after the first occurrence.
- Maximum number of logs that log suppression can operate on—When log suppression is enabled, Intrusion Detection and Prevention (IDP) must cache log records so that it can identify when multiple occurrences of the same event occur. You can specify how many log records are tracked simultaneously by IDP. By default, the maximum number of log records that IDP can operate on is 16,384.
- Time after which suppressed logs are reported—When log suppression is enabled, IDP maintains a count of occurrences of the same event. After the specified number of seconds have passed, IDP writes a single log entry containing the count of occurrences. By default, IDP reports suppressed logs after 5 seconds.

**Related  
Documentation**

- *IDP Monitoring and Troubleshooting Guide for Security Devices*
- [Understanding IDP Logging on page 1995](#)
- *IDP Policies Overview*

- [Understanding IDP Policy Rules](#)
- [Example: Configuring IDP Log Suppression Attributes on page 1999](#)

### [Understanding IDP Log Information Usage on the IC Series UAC Appliance](#)

---

The IC Series UAC Appliance for the Unified Access Control (UAC) appliance can use Intrusion Detection and Prevention (IDP) attack log information sent from the Juniper Networks device to apply access policies for traffic in which IDP logs indicate an attack has been detected. Using a secure channel of communication, these IDP logs are sent to the IC Series appliance directly and securely. IDP attack logs are sent to the IC Series appliance through the JUEP communication channel.

This topic contains the following sections:

- [Message Filtering to the IC Series UAC Appliance on page 1997](#)
- [Configuring IC Series UAC Appliance Logging on page 1997](#)

#### **Message Filtering to the IC Series UAC Appliance**

When you configure the IC Series UAC Appliance to receive IDP log messages, you set certain filtering parameters on the IC Series appliance. Without this filtering, the IC Series appliance could potentially receive too many log messages. The filtering parameters could include the following:

- The IC Series appliance should only receive communications from IDP for sessions it has authenticated. See the *Unified Access Control Administration Guide* for details.
- You can create IC Series appliance filters for receiving IDP logs files based on the their severity. For example, if on the IC Series appliance the severity is set to high, then IDP only sends logs which have a severity greater than or equal to high. See the *Unified Access Control Administration Guide* for details.
- From the IC Series appliance, you can disable the receiving of all IDP logs. See the *Unified Access Control Administration Guide* for details.

#### **Configuring IC Series UAC Appliance Logging**

All the configuration for receiving and filtering IDP logs is done on the IC Series UAC Appliance. You should refer to the *Unified Access Control Administration Guide* for configuration information for receiving IDP logs and details on the JUEP communication channel.

#### **Related Documentation**

- [IDP Monitoring and Troubleshooting Guide for Security Devices](#)
- [Understanding IDP Log Suppression Attributes on page 1996](#)
- [Understanding IDP Logging on page 1995](#)
- [Understanding Application-Level DDoS Logging](#)

#### **Packet Capture**

- [Understanding Security Packet Capture on page 1998](#)

## Understanding Security Packet Capture

---

Viewing packets that precede and follow an attack helps you determine the purpose and extent of an attempted attack, whether an attack was successful, and if any network damage was caused by an attack. Packet analysis also aids in defining attack signatures to minimize false positives.

If packet capture is enabled when an attack is logged, a specified number of packets before and after the attack can be captured for the session. When all packets have been collected, they are transmitted in Device Management Interface (DMI) to a host device for offline analysis.

A notification option in the IDP policy rule enables packet capture when a rule match occurs. The option further defines the number of packets to be captured and the duration of packet capture for the associated session.

An IDP sensor configuration defines the device specifications for the packet capture. Options for this command determine the memory to be allocated for packet capture, and the source and host devices between which the packet capture object will be transmitted.

A **show** command displays packet capture counters that provide details about the progress, success, and failure of packet capture activity on the device.

Support for packet capture is available only once on each session.

### Related Documentation

- *IDP Monitoring and Troubleshooting Guide for Security Devices*
- [Understanding IDP Logging on page 1995](#)
- [Example: Configuring Security Packet Capture on page 2177](#)

## Tuning

- [Performance and Capacity Tuning for IDP Overview on page 1998](#)

## Performance and Capacity Tuning for IDP Overview

---

This topic provides an overview on performance and capacity tuning for an Intrusion Detection and Prevention (IDP) session.

If you are deploying IDP policies, you can configure the device to increase IDP session capacity. By using the provided commands to change the way the system allocates resources, you can achieve higher IDP session capacity.

By using the **maximize-idp-sessions** command, you can increase the IDP session capacity. In this mode, by default, the device assigns a greater weight value to firewall functions. Based on your IDP policy, you can shift the weight to IDP functions to maximize IDP performance. By shifting weight, you are increasing capacity and allocating more processing power for the given service.





**NOTE:** You should not configure the device to increase IDP session capacity if you are not using an IDP policy.

The device ships with an implicit default session capacity setting. This default value adds weight to firewall sessions. You can manually override the default by adding the **maximize-idp-sessions** setting to your configuration. When you do this, in addition to IDP session scaling, you can choose to assign weight values of equal, firewall, or IDP to firewall and IDP functions. Typically, when you only include IDP-recommended attacks or client-to-server attacks in your IDP policy, IDP functions consume less CPU resources, for this reason, you would select weight firewall to maximize device performance. Alternatively, if you add server-to-client attacks to your IDP policy, IDP functions consume higher CPU resources. For this reason, you would select weight IDP to maximize performance. Essentially, you will need to configure the weight based on the desired IDP policy and performance. You do this by examining the CPU resource utilization on the packet forwarding engine by using the **show security monitoring fpc number** command.

#### Related Documentation

- [IDP Policies Overview](#)
- [Configuring Session Capacity for IDP \(CLI Procedure\) on page 2182](#)
- [IDP Monitoring and Troubleshooting Guide for Security Devices](#)

## Configuration

- [IDP Logging on page 1999](#)
- [Configuration Statements on page 2000](#)

### IDP Logging

- [Example: Configuring IDP Log Suppression Attributes on page 1999](#)

#### Example: Configuring IDP Log Suppression Attributes

This example shows how to configure log suppression attributes.

##### Requirements

Before you begin:

- Configure network interfaces.
- Download the signature database. See *Updating the IDP Signature Database Manually Overview*.

##### Overview

Log suppression ensures that minimal numbers of logs are generated for the same event or attack that occurs multiple times. Log suppression is enabled by default. You can configure certain log suppression attributes to suppress logs according to your needs.

In this example, you configure log suppression to begin after the second occurrence of an event and specify that logs are reported after 20 seconds.

### Configuration

#### Step-by-Step Procedure

To configure log suppression attributes:

1. Specify the log number after which you want to start log suppression.  

```
[edit]  
user@host# set security idp sensor-configuration log suppression start-log 2
```
2. Specify the maximum time after which suppressed logs are reported.  

```
[edit]  
user@host# set security idp sensor-configuration log suppression max-time-report 20
```
3. If you are done configuring the device, commit the configuration.  

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

### Verification

To verify log statistics, enter the **show security idp counters log** command.

#### Related Documentation

- [Updating the IDP Signature Database Manually Overview](#)
- [Example: Defining Rules for an IDP IPS Rulebase](#)
- [Understanding IDP Log Suppression Attributes on page 1996](#)
- [IDP Monitoring and Troubleshooting Guide for Security Devices](#)

## Configuration Statements

- [Security Configuration Statement Hierarchy on page 2005](#)
- [\[edit security idp\] Hierarchy Level on page 2007](#)
- [ack-number on page 2017](#)
- [action \(Security Application-Level DDoS\) on page 2018](#)
- [action \(Security Rulebase IPS\) on page 2019](#)
- [active-policy on page 2020](#)
- [action-profile on page 2021](#)
- [alert on page 2022](#)
- [allow-icmp-without-flow on page 2022](#)
- [anomaly on page 2023](#)
- [application \(Security Custom Attack\) on page 2023](#)
- [application \(Security Application-Level DDoS\) on page 2024](#)
- [application \(Security IDP\) on page 2024](#)
- [application-ddos on page 2025](#)

- [application-identification](#) on page 2026
- [attack-type \(Security Anomaly\)](#) on page 2027
- [attack-type \(Security Chain\)](#) on page 2028
- [attack-type \(Security IDP\)](#) on page 2030
- [attack-type \(Security Signature\)](#) on page 2034
- [attacks \(Security Exempt Rulebase\)](#) on page 2038
- [attacks \(Security IPS Rulebase\)](#) on page 2039
- [automatic \(Security\)](#) on page 2040
- [cache-size \(Security\)](#) on page 2040
- [category \(Security Dynamic Attack Group\)](#) on page 2041
- [chain](#) on page 2042
- [code](#) on page 2043
- [content-decompression-max-memory-kb](#) on page 2044
- [content-decompression-max-ratio](#) on page 2045
- [context \(Security Custom Attack\)](#) on page 2045
- [count \(Security Custom Attack\)](#) on page 2046
- [custom-attack](#) on page 2047
- [custom-attack-group](#) on page 2052
- [custom-attack-groups \(Security IDP\)](#) on page 2052
- [custom-attacks](#) on page 2053
- [data-length](#) on page 2053
- [datapath-debug](#) on page 2054
- [description \(Security IDP Policy\)](#) on page 2055
- [destination \(Security IP Headers Attack\)](#) on page 2056
- [destination-address \(Security IDP Policy\)](#) on page 2057
- [destination-except](#) on page 2058
- [destination-port \(Security Signature Attack\)](#) on page 2058
- [detect-shellcode](#) on page 2059
- [detector](#) on page 2059
- [direction \(Security Custom Attack\)](#) on page 2060
- [direction \(Security Dynamic Attack Group\)](#) on page 2061
- [download-timeout](#) on page 2062
- [dynamic-attack-group](#) on page 2063
- [dynamic-attack-groups \(Security IDP\)](#) on page 2064
- [enable-all-qmodules](#) on page 2064
- [enable-packet-pool](#) on page 2065
- [expression](#) on page 2065

- [false-positives](#) on page 2066
- [filters](#) on page 2067
- [flow \(Security IDP\)](#) on page 2068
- [from-zone \(Security IDP Policy\)](#) on page 2068
- [global \(Security IDP\)](#) on page 2069
- [group-members](#) on page 2070
- [header-length](#) on page 2071
- [host \(Security IDP Sensor Configuration\)](#) on page 2071
- [icmp \(Security IDP Custom Attack\)](#) on page 2072
- [icmp \(Security IDP Signature Attack\)](#) on page 2073
- [icmpv6 \(Security IDP\)](#) on page 2074
- [identification \(Security ICMP Headers\)](#) on page 2074
- [identification \(Security IP Headers\)](#) on page 2075
- [idp \(Application Services\)](#) on page 2075
- [idp \(Security Alarms\)](#) on page 2076
- [idp-policy \(Security\)](#) on page 2077
- [ignore-memory-overflow](#) on page 2079
- [ignore-reassembly-overflow](#) on page 2080
- [ignore-regular-expression](#) on page 2080
- [include-destination-address](#) on page 2081
- [install](#) on page 2081
- [interval \(Security IDP\)](#) on page 2082
- [ip \(Security IDP Custom Attack\)](#) on page 2082
- [ip-action \(Security Application-Level DDoS\)](#) on page 2083
- [ip-action \(Security IDP Rulebase IPS\)](#) on page 2084
- [ip-block](#) on page 2085
- [ip-close](#) on page 2085
- [ip-connection-rate-limit](#) on page 2086
- [ip-flags](#) on page 2087
- [ip-notify](#) on page 2087
- [ips](#) on page 2088
- [ipv4 \(Security IDP Signature Attack\)](#) on page 2089
- [ipv6 \(Security IDP\)](#) on page 2090
- [key-protection \(Security IDP Sensor Configuration\)](#) on page 2090
- [log \(Security IDP\)](#) on page 2091
- [log \(Security IDP Policy\)](#) on page 2091
- [log-attacks](#) on page 2092

- [log-create](#) on page 2092
- [log-errors](#) on page 2093
- [log-supercede-min](#) on page 2093
- [match \(Security IDP Policy\)](#) on page 2094
- [match \(Security Rulebase DDoS\)](#) on page 2095
- [max-flow-mem](#) on page 2095
- [max-logs-operate](#) on page 2096
- [max-packet-mem-ratio](#) on page 2096
- [max-packet-memory-ratio](#) on page 2097
- [max-reass-packet-memory-ratio](#) on page 2097
- [max-sessions \(Security Packet Log\)](#) on page 2098
- [max-tcp-session-packet-memory](#) on page 2098
- [max-time-report](#) on page 2099
- [max-timers-poll-ticks](#) on page 2099
- [max-udp-session-packet-memory](#) on page 2100
- [member \(Security IDP\)](#) on page 2100
- [mss \(Security IDP\)](#) on page 2101
- [negate](#) on page 2101
- [nested-application \(Security IDP\)](#) on page 2102
- [notification](#) on page 2102
- [option \(Security IDP\)](#) on page 2103
- [order \(Security IDP\)](#) on page 2103
- [packet-log \(Security IDP Policy\)](#) on page 2104
- [packet-log \(Security IDP Sensor Configuration\)](#) on page 2105
- [pattern \(Security IDP\)](#) on page 2105
- [performance](#) on page 2106
- [policy-lookup-cache](#) on page 2106
- [post-attack](#) on page 2107
- [post-attack-timeout](#) on page 2107
- [pre-attack](#) on page 2108
- [pre-filter-shellcode](#) on page 2108
- [predefined-attack-groups](#) on page 2109
- [predefined-attacks](#) on page 2109
- [process-ignore-s2c](#) on page 2110
- [process-override](#) on page 2110
- [process-port](#) on page 2111
- [products](#) on page 2111

- [protocol-binding on page 2112](#)
- [protocol-name on page 2113](#)
- [protocol \(Security IDP IP Headers\) on page 2114](#)
- [protocol \(Security IDP Signature Attack\) on page 2115](#)
- [re-assembler on page 2118](#)
- [recommended-action on page 2119](#)
- [refresh-timeout on page 2119](#)
- [regexp on page 2120](#)
- [reject-timeout on page 2120](#)
- [reset \(Security IDP\) on page 2121](#)
- [reset-on-policy on page 2121](#)
- [rpc on page 2122](#)
- [rule \(Security Exempt Rulebase\) on page 2123](#)
- [rule \(Security DDoS Rulebase\) on page 2124](#)
- [rule \(Security IPS Rulebase\) on page 2125](#)
- [rulebase-ddos on page 2127](#)
- [rulebase-exempt on page 2128](#)
- [rulebase-ips on page 2129](#)
- [scope \(Security IDP Chain Attack\) on page 2130](#)
- [scope \(Security IDP Custom Attack\) on page 2131](#)
- [security-package on page 2132](#)
- [sensor-configuration on page 2133](#)
- [sequence-number \(Security IDP ICMP Headers\) on page 2135](#)
- [sequence-number \(Security IDP TCP Headers\) on page 2136](#)
- [service \(Security IDP Anomaly Attack\) on page 2136](#)
- [service \(Security IDP Dynamic Attack Group\) on page 2137](#)
- [sessions on page 2137](#)
- [severity \(Security IDP Custom Attack\) on page 2138](#)
- [severity \(Security IDP Dynamic Attack Group\) on page 2139](#)
- [severity \(Security IDP IPS Rulebase\) on page 2140](#)
- [shellcode on page 2141](#)
- [signature \(Security IDP\) on page 2142](#)
- [source \(Security IDP IP Headers\) on page 2146](#)
- [source-address \(Security IDP Policy\) on page 2147](#)
- [source-address \(Security IDP Sensor Configuration\) on page 2147](#)
- [source-except on page 2148](#)
- [source-port \(Security IDP\) on page 2148](#)

- [ssl-inspection on page 2149](#)
- [start-log on page 2149](#)
- [start-time \(Security IDP\) on page 2150](#)
- [statistics \(Security IDP\) on page 2150](#)
- [suppression on page 2151](#)
- [target \(Security IDP\) on page 2152](#)
- [tcp \(Security IDP Protocol Binding\) on page 2153](#)
- [tcp \(Security IDP Signature Attack\) on page 2154](#)
- [tcp-flags on page 2156](#)
- [terminal on page 2157](#)
- [test \(Security IDP\) on page 2157](#)
- [then \(Security IDP Policy\) on page 2158](#)
- [then \(Security Rulebase DDos\) on page 2159](#)
- [time-binding on page 2160](#)
- [timeout \(Security IDP Policy\) on page 2160](#)
- [to-zone \(Security IDP Policy\) on page 2161](#)
- [tos on page 2162](#)
- [total-length on page 2163](#)
- [total-memory on page 2163](#)
- [traceoptions \(Security Datapath Debug\) on page 2164](#)
- [traceoptions \(Security IDP\) on page 2166](#)
- [ttl \(Security IDP\) on page 2168](#)
- [tunable-name on page 2169](#)
- [tunable-value on page 2170](#)
- [type \(Security IDP Dynamic Attack Group\) on page 2170](#)
- [type \(Security IDP ICMP Headers\) on page 2171](#)
- [udp \(Security IDP Protocol Binding\) on page 2172](#)
- [udp \(Security IDP Signature Attack\) on page 2173](#)
- [urgent-pointer on page 2174](#)
- [url \(Security IDP\) on page 2174](#)
- [window-scale on page 2175](#)
- [window-size on page 2176](#)

---

### 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 J Series and 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 59](#)
- [\[edit security alarms\] Hierarchy Level on page 1312](#)
- *[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 752](#)
- [\[edit security datapath-debug\] Hierarchy Level on page 1313](#)
- *[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 74](#)
- [\[edit security ike\] Hierarchy Level on page 83](#)
- [\[edit security ipsec\] Hierarchy Level on page 85](#)
- *[edit security log] Hierarchy Level*
- [\[edit security nat\] Hierarchy Level on page 64](#)
- *[edit security pki] Hierarchy Level*
- [\[edit security policies\] Hierarchy Level on page 59](#)
- *[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 752](#)
- [\[edit security traceoptions\] Hierarchy Level on page 1314](#)
- *[edit security user-identification] Hierarchy Level*



- [\[edit security utm\] Hierarchy Level on page 67](#)
- [\[edit security zones\] Hierarchy Level on page 87](#)

**Related  
Documentation**

- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *CLI User Guide*

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

```

security {
  idp {
    active-policy policy-name;
    application-ddos application-name {
      connection-rate-threshold number;
      context context-name {
        exclude-context-values [value];
        hit-rate-threshold number;
        max-context-values number;
        time-binding-count number;
        time-binding-period seconds;
        value-hit-rate-threshold number;
      }
      service service-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;
            }
            nested-application nested-application-name;
          }
        }
      }
    }
  }
}

```

```
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 {
      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 {
  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;
  }
  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;
    }
    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;
    }
    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;
  }
  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 {
  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;
    }
    nested-application nested-application-name;
    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-ddos {
        rule rule-name {
            description text;
            match {
                application (application-name | any | default);
                application-ddos <application-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);
            }
            then {
                action {
                    (close-server | drop-connection | drop-packet | no-action);
                }
                ip-action {
                    (ip-block | ip-close | ip-connection-rate-limit connections-per-second |
                     ip-notify);
                    log;
                    log-create;
                    refresh-timeout;
                    timeout seconds;
                }
                notification {
                    log-attacks {
                        alert;
                    }
                }
            }
        }
    }
}
}
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-ddos {
    statistics {
      interval minutes;
    }
  }
}
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);
  fifo-max-size value;
  hash-table-size value;
  (log-errors | no-log-errors);
  max-timers-poll-ticks 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);
    (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 percentage-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 58](#)
- *IDP Signature Database Feature Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*
- *IDP SSL Inspection Feature Guide for Security Devices*
- *Master Administrator for Logical Systems Feature Guide for Security Devices*
- *IDP Class of Service Action Feature Guide for Security Devices*

## ack-number

---

<b>Syntax</b>	<pre>ack-number {     match (equal   greater-than   less-than   not-equal);     value <i>acknowledgement-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the ACK number of the packet. This number identifies the next sequence number; the ACK flag must be set to activate this field.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value <i>acknowledgement-number</i></b>—Match the ACK number of the packet.</li></ul> <p><b>Range:</b> 0 through 4,294,967,295</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li></ul>

## action (Security Application-Level DDoS)

---

<b>Syntax</b>	<pre>action {     (close-server   drop-connection   drop-packet   no-action); }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the actions you want IDP to take when the monitored traffic matches the application-ddos objects specified in the application-level DDoS rule.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>close-server</b>—Closes the connection and sends an RST packet to the server but not to the client.</li><li>• <b>drop-connection</b>—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</li><li>• <b>drop-packet</b>—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.</li><li>• <b>no-action</b>—No action is taken. Use this action when you want to only generate logs for some traffic.</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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## action (Security Rulebase IPS)

<b>Syntax</b>	<pre> action {   class-of-service {     dscp-code-point <i>number</i>;     forwarding-class <i>forwarding-class</i>;   }   (close-client   close-client-and-server   close-server   drop-connection   drop-packet      ignore-connection   mark-diffserv <i>value</i>   no-action   recommended); }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the actions you want IDP to take when the monitored traffic matches the attack objects specified in the rules.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>class-of-service</b>—Associates a class-of-service forwarding class as an action to the IDP policy; also sets the value of the DSCP code point. You can use the default forwarding class names or define new ones. Forwarding-class and dscp-code-point are optional, but one must be set.</li> <li>• <b>close-client</b>—Closes the connection and sends an RST packet to the client but not to the server.</li> <li>• <b>close-client-and-server</b>—Closes the connection and sends an RST packet to both the client and the server.</li> <li>• <b>close-server</b>—Closes the connection and sends an RST packet to the server but not to the client.</li> <li>• <b>drop-connection</b>—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</li> <li>• <b>drop-packet</b>—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.</li> <li>• <b>ignore-connection</b>—Stops scanning traffic for the rest of the connection if an attack match is found. IDP disables the rulebase for the specific connection.</li> <li>• <b>mark-diffserv <i>value</i></b>—Assigns the indicated service-differentiation value to the packet in an attack, then passes them on normally.</li> <li>• <b>no-action</b>—No action is taken. Use this action when you want to only generate logs for some traffic.</li> <li>• <b>recommended</b>—All predefined attack objects have a default action associated with them. This is the action that Juniper Networks recommends when that attack is detected.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Class of Service Action Feature Guide for Security Devices</i></li></ul>

---

## active-policy

---

<b>Syntax</b>	active-policy <i>policy-name</i> ;
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify which policy among the configured policies to activate.
<b>Options</b>	<i>policy-name</i> —Name of the active policy.



**NOTE:** You need to make sure the active policy is enforced in the data plane.

---

<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></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.

<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>• <i>Network Monitoring and Troubleshooting Guide for Security Devices</i></li><li>• <a href="#">Example: Configuring Packet Capture for Datapath Debugging on page 1289</a></li></ul>

---

## alert

<b>Syntax</b>	alert;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then notification] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Set an alert flag in the Alert column of the Log Viewer for the matching log record.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

---

## allow-icmp-without-flow

<b>Syntax</b>	(allow-icmp-without-flow   no-allow-icmp-without-flow);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration flow]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Allow an ICMP packet without matched request. By default the ICMP flow is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## anomaly

---

<b>Syntax</b>	<pre> anomaly {   direction (any   client-to-server   server-to-client);   service <i>service-name</i>;   shellcode (all   intel   no-shellcode   sparc);   test <i>test-condition</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Protocol anomaly attack objects detect abnormal or ambiguous messages within a connection according to the set of rules for the particular protocol being used.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## application (Security Custom Attack)

---

<b>Syntax</b>	application <i>application-name</i> ;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the attack for a specified application.
<b>Options</b>	<i>application-name</i> —Name of the application.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## application (Security Application-Level DDoS)

---

<b>Syntax</b>	application ( <i>application-name</i>   any   default);
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>idp-policy-name</i> rulebase-ddos rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the application or application set name to match.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>application-name</b>—Name of the application or application set to match.</li><li>• <b>any</b>—Match all ports to the only application implied in the attack objects.</li><li>• <b>default</b>—Match default and automatically detected ports to the applications implied in the attack object.</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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## application (Security IDP)

---

<b>Syntax</b>	application <i>application-name</i> ;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify an application or an application set name to match.
<b>Options</b>	<i>application-name</i> —Name of the application.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## application-ddos

<b>Syntax</b>	<pre> application-ddos <i>application-name</i> {   connection-rate-threshold <i>number</i>;   context <i>context-name</i> {     exclude-context-values [<i>value</i>];     hit-rate-threshold <i>number</i>;     max-context-values <i>number</i>;     time-binding-count <i>number</i>;     time-binding-period <i>seconds</i>;     value-hit-rate-threshold <i>number</i>;   }   service <i>service-name</i>; } </pre>
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure application-level distributed denial-of-service (DDoS) protection.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## application-identification

---

<b>Syntax</b>	<pre>application-identification {     max-packet-memory-ratio <i>percentage-value</i>;     max-reass-packet-memory-ratio <i>percentage-value</i>;     max-tcp-session-packet-memory <i>value</i>;     max-udp-session-packet-memory <i>value</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Packet memory percentages added in Junos OS Release 12.1X44-D20.
<b>Description</b>	<p>Enable to identify the TCP/UDP application session running on nonstandard ports to match the application properties of transiting network traffic.</p> <p>Options define the allocation of IDP memory to application identification for packet and reassembler use.</p>
<b>Options</b>	The remaining statements are explained separately.
<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>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## attack-type (Security Anomaly)

---

<b>Syntax</b>	<pre>attack-type {   anomaly {     direction (any   client-to-server   server-to-client);     service <i>service-name</i>;     shellcode (all   intel   no-shellcode   sparc);     test <i>test-condition</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the type of attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## attack-type (Security Chain)

```
Syntax  attack-type {
        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;
            }
            nested-application nested-application-name;
            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);
    }
```

**Hierarchy Level** [edit security idp custom-attack *attack-name*]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify the type of attack.



**NOTE:** In a chain attack, you can configure multiple member attacks.

In an attack, under protocol binding TCP/UDP, you can specify multiple ranges of ports.

**Options** The remaining statements are explained separately.

<b>Required Privilege</b>	security—To view this statement in the configuration.
<b>Level</b>	security-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## attack-type (Security IDP)

```

Syntax  attack-type {
        anomaly {
            direction (any | client-to-server | server-to-client);
            shellcode (all | intel | no-shellcode | sparc);
            test-condition condition-name;
        }
        signature {
            context context-name;
            direction (any | client-to-server | server-to-client);
            negate;
            pattern signature-pattern;
            protocol {
                icmp {
                    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 {
            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;
            }
            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;
    }
    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;
    }
    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;
    }
    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 {
    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;
    }
    nested-application nested-application-name;
    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);
}

```

<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain member <i>member-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the type of attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## attack-type (Security Signature)

```

Syntax  attack-type {
        signature {
            context context-name;
            direction (any | client-to-server | server-to-client);
            negate;
            pattern signature-pattern;
            protocol {
                icmp {
                    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 {
            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;
            }
            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;
    }
    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;
    }
    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;
    }
    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 {
    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;
  }
  nested-application nested-application-name;
  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);
}
}

```

<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the type of attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## attacks (Security Exempt Rulebase)

---

<b>Syntax</b>	<pre>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]; }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the attacks that you do not want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## attacks (Security IPS Rulebase)

<b>Syntax</b>	<pre>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]; }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the attacks you want the device to match in the monitored network traffic. Each attack is defined as an attack object, which represents a known pattern of attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## automatic (Security)

---

<b>Syntax</b>	<pre>automatic {   download-timeout <i>minutes</i>;   enable;   interval <i>hours</i>;   start-time <i>start-time</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp security-package]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable the device to automatically download the updated signature database from the specified URL.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li></ul>

## cache-size (Security)

---

<b>Syntax</b>	<pre>cache-size <i>size</i>;</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the size in bytes for each user's log cache.
<b>Options</b>	<b>size</b> —Cache size. <b>Range:</b> 1 through 65,535 bytes <b>Default:</b> 12800 bytes
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## category (Security Dynamic Attack Group)

---

<b>Syntax</b>	<pre>category {     values [category-value]; }</pre>
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a category filter to add attack objects based on the category.
<b>Options</b>	<b>values</b> —Name of the category filter. You can configure multiple filters separated by spaces and enclosed in square brackets.
<b>Required Privilege Level</b>	<b>security</b> —To view this statement in the configuration. <b>security-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## chain

**Syntax**

```
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;
    }
    nested-application nested-application-name;
    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);
}
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Chain attack object combines multiple signatures and/or protocol anomalies into a single object. Traffic must match all of the combined signatures and/or protocol anomalies to match the chain attack object.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*


## code

---

<b>Syntax</b>	code { match (equal   greater-than   less-than   not-equal); value <i>code-value</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol icmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the secondary code that identifies the function of the request/reply within a given type.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>code-value</i>—Match a decimal value.</li> </ul> <p><b>Range:</b> 0 through 255</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## content-decompression-max-memory-kb

---

<b>Syntax</b>	content-decompression-max-memory-kb <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Set the maximum memory allocation in kilobytes for content decompression.</p> <p>The default memory allocation provides 33 KB per session for an average number of sessions requiring decompression at the same time. To determine if this value is consistent with your environment, analyze values from decompression-related counters and the total number of IDP sessions traversing the device. Estimate the number of sessions requiring decompression at the same time. Assuming that each of these sessions requires 33 KB of memory for decompression, compare your estimated needs to the default value.</p>
	<div> <b>NOTE:</b> Because content decompression requires a significant allocation of memory, system performance will be impacted by increasing the maximum memory allocation for decompression.</div>
<b>Options</b>	<b>Range:</b> 50 through 2,000,000 KB
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## content-decompression-max-ratio

<b>Syntax</b>	<code>content-decompression-max-ratio <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Set the maximum decompression ratio of the size of decompressed data to the size of compressed data.</p> <p>Some attacks are introduced through compressed content. When the content is decompressed, it can inflate to a very large size taking up valuable system resources resulting in denial of service. This type of attack can be recognized by the ratio of the size of decompressed data to the size of compressed data. Keep in mind, however, that a higher ratio lessens the chance of detecting this type of attack.</p>
<b>Options</b>	<b>Range:</b> 1 through 128
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## context (Security Custom Attack)

<b>Syntax</b>	<code>context <i>context-name</i>;</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Define the location of the signature where IDP should look for the attack in a specific Application Layer protocol.
<b>Options</b>	<b><i>context-name</i></b> —Name of the context under which the attack has to be matched.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## count (Security Custom Attack)

---

<b>Syntax</b>	<code>count <i>count-value</i>;</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> time-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the number of times that IDP detects the attack within the specified scope before triggering an event.
<b>Options</b>	<i>count-value</i> —Number of times IDP detects the 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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## custom-attack

```

Syntax  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;
                }
                nested-application nested-application-name;
                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 {
                    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 {
    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;
    }
    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;
}
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;
    }
    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;
    }
    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 {
    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;
    }
    nested-application nested-application-name;
    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);
}
}

```

<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement modified in Junos OS Release 9.3.
<b>Description</b>	Configure custom attack objects to detect a known or unknown attack that can be used to compromise your network.
<b>Options</b>	<p><b><i>attack-name</i></b>—Name of the custom attack object.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## custom-attack-group

---

<b>Syntax</b>	<code>custom-attack-group <i>custom-attack-group-name</i> {     group-members [<i>attack-or-attack-group-name</i>]; }</code>
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure custom attack group. A custom attack group is a list of attacks that would be matched on the traffic if the group is selected in a policy.
<b>Options</b>	<i>custom-attack-group-name</i> —Name of the custom attack group.  The remaining statement is explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## custom-attack-groups (Security IDP)

---

<b>Syntax</b>	<code>custom-attack-groups <i>attack-group-name</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match attacks] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match attacks]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a name for the custom attack group.
<b>Options</b>	<i>attack-group-name</i> —Name of the custom attack group.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## custom-attacks

<b>Syntax</b>	<code>custom-attacks [attack-name];</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match attacks], [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match attacks]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Select custom attacks defined under [edit security idp custom-attack] by specifying their names.
<b>Options</b>	<b>attack-name</b> —Name of the new custom attack object.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## data-length

<b>Syntax</b>	<pre>data-length {   match (equal   greater-than   less-than   not-equal);   value tcp-data-length; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol udp] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol icmp] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the number of bytes in the data payload. In the TCP header, for SYN, ACK, and FIN packets, this field should be empty.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value data-length</b>—Match the number of bytes in the data payload.</li> </ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></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.
<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>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li> </ul>

## description (Security IDP Policy)

<b>Syntax</b>	description text;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> ] [edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> ] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> ]
<b>Release Information</b>	Statement modified in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify descriptive text for an exempt rule, or IPS rule.
<b>Options</b>	<b>text</b> —Descriptive text about an exempt rule, or IPS rule.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## destination (Security IP Headers Attack)

---

<b>Syntax</b>	<pre>destination {     match (equal   greater-than   less-than   not-equal);     value <i>ip-address-or-hostname</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv6]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the IP address of the attack target.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>ip-address-or-hostname</i>—Match an IP address or a hostname.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## destination-address (Security IDP Policy)

<b>Syntax</b>	<code>destination-address ([<i>address-name</i>]   any   any-ipv4   any-ipv6);</code>
<b>Hierarchy Level</b>	<code>[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> match]</code> <code>[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match]</code> <code>[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a destination IP address or IP address set object to be used as the match destination address object. The default value is any.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b><i>address-name</i></b>—IP address or IP address set object.</li> <li>• <b><i>any</i></b>—Specify any IPv4 or IPv6 address.</li> <li>• <b><i>any-ipv4</i></b>—Specify any IPv4 address.</li> <li>• <b><i>any-ipv6</i></b>—Specify any IPv6 address.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## destination-except

<b>Syntax</b>	<code>destination-except [address-name];</code>
<b>Hierarchy Level</b>	<code>[edit security idp idp-policy policy-name rulebase-ddos rule rule-name match]</code> <code>[edit security idp idp-policy policy-name rulebase-exempt rule rule-name match]</code> <code>[edit security idp idp-policy policy-name rulebase-ips rule rule-name match]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a destination IP address or IP address set object to specify all destination address objects except the specified address objects. The default value is any.
<b>Options</b>	<b>address-name</b> —IP address or IP address set object.
<b>Required Privilege Level</b>	<b>security</b> —To view this statement in the configuration. <b>security-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## destination-port (Security Signature Attack)

<b>Syntax</b>	<pre>destination-port {   match (equal   greater-than   less-than   not-equal);   value destination-port; }</pre>
<b>Hierarchy Level</b>	<code>[edit security idp custom-attack attack-name attack-type signature protocol udp]</code> <code>[edit security idp custom-attack attack-name attack-type signature protocol tcp]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the port number of the attack target.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match (equal   greater-than   less-than   not-equal)</b>—Match an operand.</li> <li>• <b>value destination-port</b>—Match the port number of the attack target.</li> </ul>
	<b>Range:</b> 0 through 65,535
<b>Required Privilege Level</b>	<b>security</b> —To view this statement in the configuration. <b>security-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## detect-shellcode

<b>Syntax</b>	(detect-shellcode   no-detect-shellcode);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable to detect the shell code and prevent buffer overflow attacks. By default this setting is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## detector

<b>Syntax</b>	<pre> detector {   protocol-name <i>protocol-name</i> {     tunable-name <i>tunable-name</i> {       tunable-value <i>protocol-value</i>;     }   } } </pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure protocol detector engine for a specific service.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> <li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li> </ul>

## direction (Security Custom Attack)

---

<b>Syntax</b>	direction (any   client-to-server   server-to-client);
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type anomaly] [edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Define the connection direction of the attack.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>any</b>—Detect the attack in either direction.</li><li>• <b>client-to-server</b>—Detect the attack only in client-to-server traffic.</li><li>• <b>server-to-client</b>—Detect the attack only in server-to-client traffic.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## direction (Security Dynamic Attack Group)

<b>Syntax</b>	<pre>direction {   expression (and   or);   values [any client-to-server exclude-any exclude-client-to-server exclude-server-to-client   server-to-client]; }</pre>
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <b>expression</b> option added in Junos OS Release 11.4.
<b>Description</b>	Specify a direction filter to add predefined attacks to the dynamic group based on the direction specified in the attacks.
<b>Options</b>	<p><b>expression</b>—Boolean operators:</p> <ul style="list-style-type: none"> <li>• <b>and</b>— If both the member name patterns match, the expression matches.</li> <li>• <b>or</b>— If either of the member name patterns match, the expression matches.</li> </ul> <p><b>values</b>—Name of the direction filter. You can select from the following directions:</p> <ul style="list-style-type: none"> <li>• <b>any</b>—Monitors traffic from client to server and server to client.</li> <li>• <b>client-to-server</b>—Monitors traffic from client to server (most attacks occur over <b>client-to-server</b> connections) only.</li> <li>• <b>exclude-any</b>—Allows traffic from client to server and server to client.</li> <li>• <b>exclude-client-to-server</b>—Allows traffic from client to server only.</li> <li>• <b>exclude-server-to-client</b>—Allows traffic from server to client only.</li> <li>• <b>server-to-client</b>—Monitors traffic from server to client only.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## download-timeout

---

<b>Syntax</b>	download-timeout <i>minutes</i> ;
<b>Hierarchy Level</b>	[edit security idp security-package automatic]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6R3.
<b>Description</b>	Specify the time that the device automatically times out and stops downloading the updated signature database from the specified URL.



**NOTE:** The default value for download-timeout is one minute. If download is completed before the download times out, the signature is automatically updated after the download. If the download takes longer than the configured period, the automatic signature update is aborted.

**Options** *minutes*—Time in minutes.  
**Range:** 1 through 60 minutes  
**Default:** 1 minute



**NOTE:** For SRX Series devices the applicable range is 1 through 4,000,000 per second.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*



## dynamic-attack-group

<b>Syntax</b>	<pre>dynamic-attack-group <i>dynamic-attack-group-name</i> {   filters {     category {       values [<i>category-value</i>];     }     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 [<i>product-value</i>];     }     recommended;     service {       values [<i>service-value</i>];     }     severity {       values [critical info major minor warning];     }     type {       values [anomaly signature];     }   } }</pre>
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <b>expression</b> option added in Junos OS Release 11.4.
<b>Description</b>	Configure a dynamic attack group. A dynamic attack group selects its members based on the filters specified in the group. Therefore, the list of attacks is updated (added or removed) when a new signature database is used.
<b>Options</b>	<p><b><i>dynamic-attack-group-name</i></b>—Name of the dynamic attack group.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## dynamic-attack-groups (Security IDP)

---

<b>Syntax</b>	<code>dynamic-attack-groups <i>attack-group-name</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match attacks] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match attacks]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify a name for the dynamic attack group.
<b>Options</b>	<i>attack-group-name</i> —Name of the dynamic attack group.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## enable-all-qmodules

---

<b>Syntax</b>	<code>(enable-all-qmodules   no-enable-all-qmodules);</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration global]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable all the qmodules of the global rulebase IDP security policy. By default all the qmodules are enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## enable-packet-pool

<b>Syntax</b>	(enable-packet-pool   no-enable-packet-pool);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration global]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable the packet pool to use when the current pool is exhausted. By default packet pool is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## expression

<b>Syntax</b>	expression <i>boolean-expression</i> ;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	<p>Configure the Boolean expression. The Boolean expression defines the condition for the individual members of a chain attack that will decide if the chain attack is hit.</p> <p>For standalone IDP devices, expression overrides order function.</p> <p>For SRX Series devices, expression and order cannot be configured together. Only one of them can be specified.</p>
<b>Options</b>	<p><b><i>boolean-expression</i></b>—Boolean operators:</p> <ul style="list-style-type: none"> <li>• <b>or</b>—If either of the member name patterns match, the expression matches.</li> <li>• <b>and</b>—If both of the member name patterns match, the expression matches. It does not matter which order the members appear in.</li> <li>• <b>oand</b>—If both of the member name patterns match, and if they appear in the same order as in the Boolean Expression, the expression matches.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## false-positives

---

<b>Syntax</b>	false-positives { values [frequently occasionally rarely unknown]; }
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a false positives filter to track attack objects based on the frequency that the attack produces a false positive on your network.
<b>Options</b>	<p><b>values</b>—Name of the false positives filter. You can select from the following false positive frequency:</p> <ul style="list-style-type: none"><li>• <b>frequently</b>—Frequently track false positive occurrences.</li><li>• <b>occasionally</b>—Occasionally track false positive occurrences.</li><li>• <b>rarely</b>—Rarely track false positive occurrences.</li><li>• <b>unknown</b>—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track false positives.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## filters

<b>Syntax</b>	<pre> filters {   category {     values [<i>category-value</i>];   }   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 [<i>product-value</i>];   }   recommended;   service {     values [<i>service-value</i>];   }   severity {     values [critical info major minor warning];   }   type {     values [anomaly signature];   } } </pre>
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <b>expression</b> option added in Junos OS Release 11.4.
<b>Description</b>	To create a dynamic attack group, set the criteria using different types of filters.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## flow (Security IDP)

---

<b>Syntax</b>	<pre>flow {     (allow-icmp-without-flow   no-allow-icmp-without-flow);     fifo-max-size <i>value</i>;     hash-table-size <i>value</i>;     (log-errors   no-log-errors);     max-timers-poll-ticks <i>value</i>;     reject-timeout <i>value</i>;     (reset-on-policy   no-reset-on-policy);     udp-anticipated-timeout <i>value</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the IDP engine to manage the packet flow.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## from-zone (Security IDP Policy)

---

<b>Syntax</b>	<pre>from-zone (<i>zone-name</i>   any);</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a source zone to be associated with the security policy. The default value is any.
<b>Options</b>	<b>zone-name</b> —Name of the source zone object.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## global (Security IDP)

---

<b>Syntax</b>	<pre>global {     (enable-all-qmodules   no-enable-all-qmodules);     (enable-packet-pool   no-enable-packet-pool);     gtp (decapsulation   no-decapsulation);     memory-limit-percent <i>value</i>;     (policy-lookup-cache   no-policy-lookup-cache); }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the global rulebase IDP security policy.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## group-members

---

<b>Syntax</b>	<code>group-members [attack-or-attack-group-name];</code>
<b>Hierarchy Level</b>	<code>[edit security idp custom-attack-group custom-attack-group-name]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	<p>Specify the group members in a custom group. The members can be predefined attacks, predefined attack groups, custom attacks, or custom dynamic groups.</p> <p>Use custom groups for the following tasks:</p> <ul style="list-style-type: none"><li>• To define a specific set of attacks to which you know your network is vulnerable.</li><li>• To group your custom attack objects.</li><li>• To define a specific set of informational attack objects that you use to keep you aware of what is happening on your network.</li></ul>
<b>Options</b>	<b>attack-or-attack-group-name</b> —Name of the attack object or group attack object.
<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>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## header-length

<b>Syntax</b>	header-length { match (equal   greater-than   less-than   not-equal); value <i>header-length</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the number of bytes in the TCP header.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>header-length</i>—Match the number of bytes in the TCP header.</li> </ul> <p><b>Range:</b> 0 through 15 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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## host (Security IDP Sensor Configuration)

<b>Syntax</b>	host <i>ip-address</i> <port number>;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the IP address and port number of the server where the packet capture object will be sent.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>host</b> <i>ip-address</i>—The IP address of the server where the packet capture object will be sent.</li> <li>• <b>port</b> <i>number</i>—The port number of the server where the packet capture object will be sent.</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>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>

## icmp (Security IDP Custom Attack)

---

<b>Syntax</b>	icmp;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the attack for the specified ICMP.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## icmp (Security IDP Signature Attack)

```
Syntax  icmp {
        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;
        }
    }
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Allow IDP to match the ICMP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## icmpv6 (Security IDP)

---

<b>Syntax</b>	icmpv6;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify that the attack is for ICMPv6 packets only.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## identification (Security ICMP Headers)

---

<b>Syntax</b>	identification { match (equal   greater-than   less-than   not-equal); value <i>identification-value</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol icmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a unique value used by the destination system to associate requests and replies.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>identification-value</i>—Match a decimal value.</li></ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## identification (Security IP Headers)

<b>Syntax</b>	identification { match (equal   greater-than   less-than   not-equal); value <i>identification-value</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a unique value used by the destination system to reassemble a fragmented packet.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>identification-value</i>—Match a decimal value.</li> </ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## idp (Application Services)

<b>Syntax</b>	idp;
<b>Hierarchy Level</b>	[edit security policies from-zone <i>zone-name</i> to-zone <i>zone-name</i> policy <i>policy-name</i> then permit application-services]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Configure Intrusion Detection and Prevention (IDP) for application services.
<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>• <i>IDP Policies Feature Guide for Security Devices</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>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>

## idp-policy (Security)

```
Syntax  idp-policy policy-name {
    rulebase-ddos {
        rule rule-name {
            description text;
            match {
                application (application-name | any | default);
                application-ddos <application-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);
            }
            then {
                action {
                    (close-server | drop-connection | drop-packet | no-action);
                }
                ip-action {
                    (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
                    log;
                    log-create;
                    refresh-timeout;
                    timeout seconds;
                }
                notification {
                    log-attacks {
                        alert;
                    }
                }
            }
        }
    }
}

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);
    }
  }
}
}

```



<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure a security IDP policy.
<b>Options</b>	<i>policy-name</i> —Name of the IDP policy.  The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

---

## ignore-memory-overflow

<b>Syntax</b>	(ignore-memory-overflow   no-ignore-memory-overflow);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration re-assembler]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable the TCP reassembler to ignore the memory overflow to prevent the dropping of IDP custom applications. By default this feature is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ignore-reassembly-overflow

---

<b>Syntax</b>	ignore-reassembly-overflow
<b>Hierarchy Level</b>	[edit security idp sensor-configuration re-assembler]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Enable the TCP reassembler to ignore the global reassembly overflow to prevent the dropping of application traffic. This feature is enabled by default.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ignore-regular-expression

---

<b>Syntax</b>	(ignore-regular-expression   no-ignore-regular-expression);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable regular expression to detect intrusion attempts. By default this setting is disabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## include-destination-address

---

<b>Syntax</b>	(include-destination-address   no-include-destination-address);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log suppression]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	When log suppression is enabled, multiple occurrences of events with the same source, service, and matching attack object generate a single log record with a count of occurrences. If you enable this option, log suppression will only combine log records for events with a matching source as well. The IDP Sensor does not consider destination when determining matching events for log suppression. By default this setting is disabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## install

---

<b>Syntax</b>	install { ignore-version-check; }
<b>Hierarchy Level</b>	[edit security idp security-package]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configures the <b>install</b> command.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>

## interval (Security IDP)

---

<b>Syntax</b>	<code>interval <i>hours</i>;</code>
<b>Hierarchy Level</b>	[edit security idp security-package automatic]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the amount of time that the device waits before updating the signature database. User should insert a default value.
<b>Options</b>	<b>hours</b> —Number of hours that the device waits. <b>Range:</b> 24 through 336 hours
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ip (Security IDP Custom Attack)

---

<b>Syntax</b>	<pre>ip {   protocol-number <i>transport-layer-protocol-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the attack for a specified IP protocol type.
<b>Options</b>	<b>protocol-number <i>transport-layer-protocol-number</i></b> —Transport Layer protocol number. <b>Range:</b> 0 through 139
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>


---

## ip-action (Security Application-Level DDoS)

---

<b>Syntax</b>	<pre>ip-action {   (ip-block   ip-close   ip-connection-rate-limit <i>connections-per-second</i>   ip-notify);   log;   log-create;   refresh-timeout;   timeout <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the actions you want IDP to take against future connections that use the same IP address.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ip-action (Security IDP Rulebase IPS)

<b>Syntax</b>	<pre> 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 <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the actions you want IDP to take against future connections that use the same IP address.
<b>Options</b>	The remaining statements are explained separately.
<div style="display: flex; align-items: center; margin-top: 20px;">  <div> <p><b>NOTE:</b> For ICMP flows, the destination port is 0; therefore, any ICMP flow matching source port, source address, and destination address is blocked.</p> </div> </div>	
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## ip-block

<b>Syntax</b>	ip-block;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Block future connections of any session that matches the IP action. If there is an IP action match with multiple rules, then the most severe IP action of all the matched rules is applied. The highest IP action priority (that is, the most severe action) is Drop/Block, then Close, then Notify.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## ip-close

<b>Syntax</b>	ip-close;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Close future connections of any new sessions that match the IP action by sending RST packets to the client and server.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## ip-connection-rate-limit

---

<b>Syntax</b>	<code>ip-connection-rate-limit <i>connections-per-second</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	When a match is made in a rulebase-ddos rule you can set the <b>then</b> action to <code>ip-connection-rate-limit</code> , which will limit the rate of future connections based on a connections per second limit that you set. This can be used to reduce the number of attacks from a client.
<b>Options</b>	<b>value</b> —Defines the connection rate limit per second on the matched host. <b>Range:</b> 1 to the maximum connections per second capability of the device.
<b>Required Privilege Level</b>	<b>security</b> —To view this statement in the configuration. <b>security-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## ip-flags

<b>Syntax</b>	ip-flags { (df   no-df); (mf   no-mf); (rb   no-rb); }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify that IDP looks for a pattern match whether or not the IP flag is set.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>df   no-df</b>—When set, the df (Don't Fragment) indicates that the packet cannot be fragmented for transmission. When unset, it indicates that the packet can be fragmented.</li> <li>• <b>mf   no-mf</b>—When set, the mf (More Fragments) indicates that the packet contains more fragments. When unset, it indicates that no more fragments remain.</li> <li>• <b>rb   no-rb</b>—When set, the rb (Reserved Bit) indicates that the bit is reserved.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## ip-notify

<b>Syntax</b>	ip-notify;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Do not take any action against future traffic, but do log the event.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## ips

---

<b>Syntax</b>	<pre>ips {   content-decompression-max-memory-kb <i>value</i>;   content-decompression-max-ratio <i>value</i>;   (detect-shellcode   no-detect-shellcode);   fifo-max-size <i>value</i>;   (ignore-regular-expression   no-ignore-regular-expression);   log-supercede-min <i>minimum-value</i>;   pre-filter-shellcode;   (process-ignore-s2c   no-process-ignore-s2c);   (process-override   no-process-override);   process-port <i>port-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure IPS security policy sensor settings.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ipv4 (Security IDP Signature Attack)

```
Syntax  ipv4 {
        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;
        }
        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;
        }
    }
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Allow IDP to match the IP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## ipv6 (Security IDP)

---

<b>Syntax</b>	ipv6;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify that the attack is for all IPv6 packets only.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## key-protection (Security IDP Sensor Configuration)

---

<b>Syntax</b>	key-protection;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ssl-inspection]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Enable secure key handling. This option is off by default.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>

## log (Security IDP)

<b>Syntax</b>	<pre>log {   cache-size <i>size</i>;   suppression {     disable;     (include-destination-address   no-include-destination-address);     max-logs-operate <i>value</i>;     max-time-report <i>value</i>;     start-log <i>value</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure IDP security policy logs.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## log (Security IDP Policy)

<b>Syntax</b>	log;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Log the information about the IP action against the traffic that matches a rule.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## log-attacks

---

<b>Syntax</b>	log-attacks { alert; }
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then notification] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Enable the log attacks to create a log record that appears in the log viewer.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## log-create

---

<b>Syntax</b>	log-create;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Generate a log event on installing the ip-action filter.
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## log-errors

---

<b>Syntax</b>	(log-errors   no-log-errors);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration flow]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable the error log to generate the result of success or failure about the flow. A flow-related error is when IDP receives a packet that does not fit into expected flow. By default error log is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## log-supersede-min

---

<b>Syntax</b>	log-supersede-min <i>minimum-value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the amount of time to supersede the IPS sensor logs.
<b>Options</b>	<i>minimum-value</i> —Minimum time to supersede the log. <b>Range:</b> 0 through 65,535 seconds <b>Default:</b> 1 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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## match (Security IDP Policy)

---

<b>Syntax</b>	<pre>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); }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> ] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the rules to be used as match criteria.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## match (Security Rulebase DDoS)

<b>Syntax</b>	<pre>match {   application (<i>application-name</i>   any   default);   application-ddos &lt;<i>application-name</i>&gt;;   destination-address ([<i>address-name</i>]   any   any-ipv4   any-ipv6);   destination-except [<i>address-name</i>];   from-zone (<i>zone-name</i>   any);   source-address ([<i>address-name</i>]   any   any-ipv4   any-ipv6);   source-except [<i>address-name</i>];   to-zone (<i>zone-name</i>   any); }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the rules to be used as match criteria for application-level DDoS protection.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## max-flow-mem

<b>Syntax</b>	max-flow-mem <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration re-assembler]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Define the maximum TCP flow memory that the IDP sensor can handle.
<b>Options</b>	<i>value</i> —Maximum TCP flow memory in kilobytes. <b>Range:</b> 64 through 4,294,967,295 kilobytes <b>Default:</b> 1024 kilobytes
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## max-logs-operate

---

<b>Syntax</b>	<code>max-logs-operate value;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log suppression]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	When log suppression is enabled, IDP must cache log records so that it can identify when multiple occurrences of the same event occur. This setting specifies how many log records are tracked simultaneously by IDP.
<b>Options</b>	<b>value</b> —Maximum number of log records are tracked by IDP. <b>Range:</b> 256 through 65536 records <b>Default:</b> 16384 records
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## max-packet-mem-ratio

---

<b>Syntax</b>	<code>max-packet-mem-ratio percentage-value;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration re-assembler]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D20.
<b>Description</b>	<p>By default, values for IDP reassembler packet memory are established as percentages of all memory. In most cases, these default values are adequate.</p> <p>If a deployment exhibits an excessive number of dropped TCP packets or retransmissions resulting in high IDP reassembly memory usage, use the <b>max-packet-mem-ratio</b> option to reset the percentage of available IDP memory for IDP reassembly packet memory. Acceptable values are between 5% and 40%.</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>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li></ul>

## max-packet-memory-ratio

<b>Syntax</b>	max-packet-memory-ratio <i>percentage-value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D20.
<b>Description</b>	<p>By default, the amount of IDP memory used for application identification packet memory is established as a percentage of all IDP memory. In most cases, the default value is adequate.</p> <p>If a deployment exhibits an excessive number of ignored IDP sessions due to application identification memory allocation failures, use the <b>max-packet-memory-ratio</b> option to set application identification packet memory limit at a higher percentage of available IDP memory. This memory is only used by IDP in cases where application identification delays identifying an application. Acceptable values are between 5% and 40%.</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>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>

## max-reass-packet-memory-ratio

<b>Syntax</b>	max-reass-packet-memory-ratio <i>percentage-value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.1X44-D20.
<b>Description</b>	<p>By default, the amount of IDP memory used for packet memory by the application identification reassembler is established as a percentage of all IDP memory. In most cases, the default value is adequate.</p> <p>If a deployment exhibits an excessive number of ignored IDP sessions due to packet memory limitations of the application identification reassembler, use the <b>max-reass-packet-memory-ratio</b> option to set the reassembler packet memory limit to a higher percentage of available IDP memory. Acceptable values are between 5% and 40%.</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>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>

## max-sessions (Security Packet Log)

---

<b>Syntax</b>	max-sessions <i>percentage</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the maximum number of sessions actively conducting pre-attack packet captures on a device at one time. This value is expressed as a percentage of the maximum number of IDP sessions for the device.
<b>Options</b>	<b>percentage</b> —Maximum number of packet capture sessions expressed as a percentage of the IDP session capacity for the device. <b>Range:</b> 1 to 100 percent <b>Default:</b> 10
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## max-tcp-session-packet-memory

---

<b>Syntax</b>	max-tcp-session-packet-memory <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the maximum number of TCP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new TCP sessions.
<b>Options</b>	<b>value</b> —Maximum number of TCP sessions. <b>Range:</b> 0 through 60,000
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## max-time-report

---

<b>Syntax</b>	max-time-report <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log suppression]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	When log suppression is enabled, IDP maintains a count of multiple occurrences of the same event. After the specified number of seconds has passed, IDP writes a single log entry containing the count of occurrences.
<b>Options</b>	<i>value</i> —Time after which IDP writes a single log entry containing the count of occurrences. <b>Range:</b> 1 through 60 seconds <b>Default:</b> 5 seconds
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## max-timers-poll-ticks

---

<b>Syntax</b>	max-timers-poll-ticks <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration flow]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the time at which timer ticks at regular interval.
<b>Options</b>	<i>value</i> —Maximum amount of time at which the timer ticks. <b>Range:</b> 0 through 1000 ticks <b>Default:</b> 1000 ticks
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## max-udp-session-packet-memory

---

<b>Syntax</b>	<code>max-udp-session-packet-memory value;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration application-identification]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the maximum number of UDP sessions that IDP maintains. If the sensor reaches the maximum, it drops all new UDP sessions.
<b>Options</b>	<b>value</b> —Maximum number of UDP sessions. <b>Range:</b> 0 through 20000
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## member (Security IDP)

---

<b>Syntax</b>	<pre>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);   } }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Create the list of member attacks.
<b>Options</b>	<b>member-name</b> —Name of the member list.  The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## mss (Security IDP)

<b>Syntax</b>	<pre>mss {     match (equal   greater-than   less-than   not-equal);     value <i>maximum-segment-size</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the maximum segment size (MSS) in the TCP header.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>maximum-segment-size</i>—Match the maximum segment size value.</li> </ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## negate

<b>Syntax</b>	negate;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Select negate to exclude the specified pattern from being matched.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## nested-application (Security IDP)

---

<b>Syntax</b>	<code>nested-application <i>nested-application-name</i>;</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the nested application name.
<b>Options</b>	<i>nested-application-name</i> —Name of the nested application.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## notification

---

<b>Syntax</b>	<pre>notification {   log-attacks {     alert;   }   packet-log {     post-attack <i>number</i>;     post-attack-timeout <i>seconds</i>;     pre-attack <i>number</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Added packet capture support in Junos OS Release 10.2.
<b>Description</b>	Configure the logging options against the action. When attacks are detected, you can choose to log an attack and create log records with attack information and send that information to the log server.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## option (Security IDP)

<b>Syntax</b>	option { match (equal   greater-than   less-than   not-equal); value <i>tcp-option</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the TCP option type (kind field in the TCP header).
<b>Options</b>	<p><b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</p> <p><b>value <i>tcp-option</i></b>—Match the option value.</p> <p><b>Range:</b> 0 through 255</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## order (Security IDP)

<b>Syntax</b>	order;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Create a compound attack object that must match each member signature or protocol anomaly in the order you specify. If you do not specify an ordered match, the compound attack object still must match all members, but the attacks or protocol anomalies can appear in random order.
<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>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## packet-log (Security IDP Policy)

---

<b>Syntax</b>	<pre>packet-log {     post-attack <i>number</i>;     post-attack-timeout <i>seconds</i>;     pre-attack <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	In response to a rule match, capture the packets received before and after the attack for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack, and limit the duration of post-attack packet capture by specifying a timeout value.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## packet-log (Security IDP Sensor Configuration)

<b>Syntax</b>	<pre>packet-log {     host <i>ip-address</i> &lt;port <i>number</i>&gt;;     max-sessions <i>percentage</i>;     source-address <i>ip-address</i>;     total-memory <i>percentage</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the sensor for packet capture. This configuration defines the amount of memory to be allocated for packet capture and the maximum number of sessions that can generate packet capture data for the device at one time. The configuration also identifies the source address and host address for transmission of the completed packet capture object.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## pattern (Security IDP)

<b>Syntax</b>	<code>pattern <i>signature-pattern</i>;</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the pattern IDP should match. You construct the attack pattern just as you would when creating a new signature attack object.
<b>Options</b>	<i>signature-pattern</i> —Specify the signature pattern.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## performance

---

<b>Syntax</b>	<pre>performance {   values [fast normal slow unknown]; }</pre>
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a performance filter to add attack objects based on the performance level that is vulnerable to the attack.
<b>Options</b>	<p><b>values</b>—Name of the performance filter. You can select from the following performance levels:</p> <ul style="list-style-type: none"><li>• <b>fast</b>—Fast track performance level.</li><li>• <b>normal</b>—Normal track performance level.</li><li>• <b>slow</b>—Slow track performance level.</li><li>• <b>unknown</b>—By default, all compound attack objects are set to Unknown. As you fine-tune IDP to your network traffic, you can change this setting to help you track performance level.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## policy-lookup-cache

---

<b>Syntax</b>	(policy-lookup-cache   no-policy-lookup-cache);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration global]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable cache to accelerate IDP policy lookup.
<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>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## post-attack

<b>Syntax</b>	<code>post-attack <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the number of packets received after an attack that should be captured for further analysis of attacker behavior. If post-attack packets are not significant to your analysis or the configured attack response ends packet transfer, you can set the post-attack option to 0.
<b>Options</b>	<p><b><i>number</i></b>—Number of post-attack packets to be captured.</p> <p><b>Range:</b> 0 through 255</p> <p><b>Default:</b> 1</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## post-attack-timeout

<b>Syntax</b>	<code>post-attack-timeout <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify a time limit for capturing post-attack packets for a session. No packet capture is conducted after the timeout has expired.
<b>Options</b>	<p><b><i>seconds</i></b>—Maximum number of seconds for post-attack packet capture.</p> <p><b>Range:</b> 0 through 1800 seconds</p> <p><b>Default:</b> 5</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## pre-attack

---

<b>Syntax</b>	<code>pre-attack <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then notification packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the number of packets received before an attack that should be captured for further analysis of attacker behavior.
<b>Options</b>	<i>number</i> —Number of pre-attack packets. <b>Range:</b> 1 through 255 <b>Default:</b> 1
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## pre-filter-shellcode

---

<b>Syntax</b>	<code>pre-filter-shellcode;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable to pre-filter the shell code and protects it from buffer overflow attacks. By default this setting is enabled.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## predefined-attack-groups

---

<b>Syntax</b>	<code>predefined-attack-groups [attack-group-name];</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match attacks], [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match attacks]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify predefined attack groups that you can use to match the traffic against known attack objects. You can update only the list of attack objects.
<b>Options</b>	<b>attack-name</b> —Name of the predefined attack object group.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## predefined-attacks

---

<b>Syntax</b>	<code>predefined-attacks [attack-name];</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match attacks], [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match attacks]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify predefined attack objects that you can use to match the traffic against known attacks. You can update only the list of attack objects.
<b>Options</b>	<b>attack-name</b> —Name of the predefined attack objects.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## process-ignore-s2c

---

<b>Syntax</b>	(process-ignore-s2c   no-process-ignore-s2c);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set the command to disable the server-to-client inspection.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## process-override

---

<b>Syntax</b>	(process-override   no-process-override);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set the command to forcefully run the IDS inspection module even if there is no policy match.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## process-port

---

<b>Syntax</b>	<code>process-port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ips]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set the command to a specific port to forcefully run the IDS inspection module on that TCP/UDP port even if there is no policy match.
<b>Options</b>	<p><b><i>port-number</i></b>—Port Number.</p> <p><b>Range:</b> 0 through 65,535</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## products

---

<b>Syntax</b>	<pre>products {   values [<i>product-value</i>]; }</pre>
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a products filter to add attack objects based on the application that is vulnerable to the attack.
<b>Options</b>	<b>values</b> —Name of the products filter. You can configure multiple filters separated by spaces and enclosed in square brackets.
<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>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## protocol-binding

---

<b>Syntax</b>	<pre>protocol-binding {   application <i>application-name</i>;   icmp;   icmpv6;   ip {     protocol-number <i>transport-layer-protocol-number</i>;   }   ipv6 {     protocol-number <i>transport-layer-protocol-number</i>;   }   nested-application <i>nested-application-name</i>;   rpc {     program-number <i>rpc-program-number</i>;   }   tcp {     minimum-port <i>port-number</i> &lt;maximum-port <i>port-number</i>&gt;;   }   udp {     minimum-port <i>port-number</i> &lt;maximum-port <i>port-number</i>&gt;;   } }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain] [edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Select a protocol that the attack uses to enter your network.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## protocol-name

---

<b>Syntax</b>	<pre> protocol-name <i>protocol-name</i> {     tunable-name <i>tunable-name</i> {         tunable-value <i>protocol-value</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration detector]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for file format decoding over HTTP using MIME added in Junos OS Release 11.2.
<b>Description</b>	Specify the name of the protocol to be used to configure each of the protocol detector engines.
<b>Options</b>	<p><b><i>protocol-name</i></b>—Name of the specific protocol.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> <li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li> </ul>

## protocol (Security IDP IP Headers)

---

<b>Syntax</b>	<pre>protocol {     match (equal   greater-than   less-than   not-equal);     value <i>transport-layer-protocol-id</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the Transport Layer protocol number.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>transport-layer-protocol-id</i>—Match the Transport Layer protocol ID.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## protocol (Security IDP Signature Attack)

```
Syntax  protocol {
        icmp {
            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 {
            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;
            }
            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;
    }
    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;
    }
    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;
}
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 {
    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;
    }
}
}

```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Specify a protocol to match the header information for the signature attack.

<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

---

## re-assembler

<b>Syntax</b>	<pre>re-assembler {   action-on-reassembly-failure (drop   drop-session   ignore);   (ignore-memory-overflow   no-ignore-memory-overflow);   (ignore-reassembly-memory-overflow   no-ignore-reassembly-memory-overflow);   ignore-reassembly-overflow;   max-flow-mem <i>value</i>;   max-packet-mem-ratio <i>percentage-value</i>;   (tcp-error-logging   no-tcp-error-logging); }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Packet memory ratios added in Junos OS Release 12.1X44-D20.
<b>Description</b>	Configure TCP reassembler for IDP sensor settings.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li></ul>



## recommended-action

<b>Syntax</b>	<code>recommended-action (close   close-client   close-server   drop   drop-packet   ignore   none);</code>
<b>Hierarchy Level</b>	<code>[edit security idp custom-attack <i>attack-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	When the security device detects an attack, it performs the specified action.
<b>Options</b>	<p>The seven actions are as follows, from most to least severe:</p> <ul style="list-style-type: none"> <li>• <b>close</b>—Reset the client and the server.</li> <li>• <b>close-client</b>—Reset the client.</li> <li>• <b>close-server</b>—Reset the server.</li> <li>• <b>drop</b>—Drop the particular packet and all subsequent packets of the flow.</li> <li>• <b>drop-packet</b>—Drop the particular packet of the flow.</li> <li>• <b>ignore</b>—Do not inspect any further packets.</li> <li>• <b>none</b>—Do not perform any action.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## refresh-timeout

<b>Syntax</b>	<code>refresh-timeout;</code>
<b>Hierarchy Level</b>	<p><code>[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action]</code></p> <p><code>[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]</code></p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Refresh the ip-action timeout so it does not expire when future connections match the installed ip-action filter.
<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>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## regex

---

<b>Syntax</b>	<code>regex <i>regular-expression</i>;</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a Perl Compatible Regular Expression (PCRE) expression.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## reject-timeout

---

<b>Syntax</b>	<code>reject-timeout <i>value</i>;</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration flow]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<p>Specify the amount of time in seconds within which a response must be received.</p> <p>This time-out is applied on flow when drop-connection action is taken by IPS for TCP flow.</p>
<b>Options</b>	<p><b>value</b>—Maximum amount of time in seconds.</p> <p><b>Range:</b> 1 through 65,535 seconds</p> <p><b>Default:</b> 300 seconds</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## reset (Security IDP)

---

<b>Syntax</b>	reset;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Select <b>reset</b> if the compound attack should be matched more than once within a single session or transaction.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## reset-on-policy

---

<b>Syntax</b>	(reset-on-policy   no-reset-on-policy);
<b>Hierarchy Level</b>	[edit security idp sensor-configuration flow]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	IDP keeps track of connections in a table. If enabled, the security module resets the flow table each time a security policy loads or unloads. If this setting is disabled, then the security module continues to retain a previous security policy until all flows referencing that security policy go away. Juniper Networks recommends that you keep this setting enabled to preserve memory.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## rpc

---

<b>Syntax</b>	<pre>rpc {   program-number <i>rpc-program-number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the attack for a specified remote procedure call (RPC) program number.
<b>Options</b>	<b>program-number <i>rpc-program-number</i></b> —RPC program number.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## rule (Security Exempt Rulebase)

**Syntax**

```
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);
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-exempt]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify exempt rule to create, modify, delete, and reorder the rules in a rulebase.

**Options** *rule-name*—Name of the exempt rulebase rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## rule (Security DDoS Rulebase)

```

Syntax    rule rule-name {
              description text;
              match {
                application (application-name | any | default);
                application-ddos <application-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);
              }
              then {
                action {
                  (close-server | drop-connection | drop-packet | no-action);
                }
                ip-action {
                  (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
                  log;
                  log-create;
                  refresh-timeout;
                  timeout seconds;
                }
                notification {
                  log-attacks {
                    alert;
                  }
                }
              }
            }

```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Configure application-level DDoS rule match criteria, and the action to be taken on attack clients.

**Options** *rule-name*—Name of the DDoS rulebase rule.

The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *Application-Level Distributed Denial of Service Feature Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## rule (Security IPS Rulebase)

```

Syntax  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);
        }
    }

```

Hierarchy Level [edit security idp idp-policy *policy-name* rulebase-ips]

<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify IPS rule to create, modify, delete, and reorder the rules in a rulebase.
<b>Options</b>	<p><i>rule-name</i>—Name of the IPS rulebase rule.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## rulebase-ddos

```
Syntax rulebase-ddos {
    rule rule-name {
        description text;
        match {
            application (application-name | any | default);
            application-ddos <application-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);
        }
        then {
            action {
                (close-server | drop-connection | drop-packet | no-action);
            }
            ip-action {
                (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
                log;
                log-create;
                refresh-timeout;
                timeout seconds;
            }
            notification {
                log-attacks {
                    alert;
                }
            }
        }
    }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name*]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Configure the rulebase parameters for application-level DDoS attacks.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *Application-Level Distributed Denial of Service Feature Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## rulebase-exempt

**Syntax**

```
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);
    }
  }
}
```

**Hierarchy Level** [edit security idp idp-policy *policy-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Configure the exempt rulebase to skip detection of a set of attacks in certain traffic.



**NOTE:** You must configure the IPS rulebase before configuring the exempt rulebase.

**Options** The remaining statements are explained separately.

**Required Privilege Level**  
 security—To view this statement in the configuration.  
 security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## rulebase-ips

```
Syntax 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);
        }
    }
}
```

<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the IPS rulebase to detect attacks based on stateful signature and protocol anomalies.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Class of Service Action Feature Guide for Security Devices</i></li></ul>

---

## scope (Security IDP Chain Attack)

---

<b>Syntax</b>	scope (session   transaction);
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify whether the match should occur over a single session or can be made across multiple transactions within a session.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>session</b>—Allow multiple matches for the object within the same session.</li><li>• <b>transaction</b>—Match the object across multiple transactions that occur within the same session.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## scope (Security IDP Custom Attack)

---

<b>Syntax</b>	scope (destination   peer   source);
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> time-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify whether the counting of the attack is from the same source IP address, the same destination IP address, or a peer.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>destination</b>—IDP detects attacks to a given destination IP address for the specified number of times, regardless of the source IP address.</li><li>• <b>peer</b>—IDP detects attacks between source and destination IP addresses of the sessions for the specified number of times.</li><li>• <b>source</b>—IDP detects attacks from a given source IP address for the specified number of times, regardless of the destination IP address.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## security-package

---

<b>Syntax</b>	<pre>security-package {   automatic {     download-timeout <i>minutes</i>;     enable;     interval <i>hours</i>;     start-time <i>start-time</i>;   }   install {     ignore-version-check;   }   source-address <i>address</i>;   url <i>url-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure the device to automatically download the updated signature database from the specified URL.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li></ul>

## sensor-configuration

```
Syntax  sensor-configuration {
        application-ddos {
            statistics {
                interval minutes;
            }
        }
        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);
            fifo-max-size value;
            hash-table-size value;
            (log-errors | no-log-errors);
            max-timers-poll-ticks 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;
        }
        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);
    (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 percentage-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;
}
disable-low-memory-handling;
}

```

<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Packet memory ratios added in Junos OS Release 12.1X44-D20.
<b>Description</b>	Configure various IDP parameters to match the properties of transiting network traffic.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> <li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li> <li>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>



## sequence-number (Security IDP ICMP Headers)

<b>Syntax</b>	sequence-number { match (equal   greater-than   less-than   not-equal); value <i>sequence-number</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol icmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the sequence number of the packet. This number identifies the location of the request/reply in relation to the entire sequence.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>sequence-number</i>—Match a decimal value.</li> </ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## sequence-number (Security IDP TCP Headers)

---

<b>Syntax</b>	sequence-number { match (equal   greater-than   less-than   not-equal); value <i>sequence-number</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the sequence number of the packet. This number identifies the location of the data in relation to the entire data sequence.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>sequence-number</i>—Match a decimal value.</li></ul> <p><b>Range:</b> 0 through 4,294,967,295</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## service (Security IDP Anomaly Attack)

---

<b>Syntax</b>	service <i>service-name</i> ;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type anomaly]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Service is the protocol whose anomaly is defined in the attack. IP, TCP, UDP, and ICMP are also valid as services. (Protocol names must be entered in lowercase.)
<b>Options</b>	<b><i>service-name</i></b> —Name of the protocol in lowercase.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## service (Security IDP Dynamic Attack Group)

<b>Syntax</b>	service { values [ <i>service-value</i> ]; }
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a service filter to add attack objects based on the attack service, such as FTP, HTTP, NetBios, and so on.
<b>Options</b>	<b>values</b> —Name of the service filter. You can configure multiple filters separated by spaces and enclosed in square brackets.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## sessions

<b>Syntax</b>	sessions <i>number</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration ssl-inspection]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Maximum number of SSL sessions for inspection. This limit is per Services Processing Unit (SPU).
<b>Options</b>	<b>number</b> —Number of SSL session to inspect. <b>Range:</b> 1 through 100,000 <b>Default:</b> 10,000
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> <li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li> </ul>

## severity (Security IDP Custom Attack)

---

<b>Syntax</b>	severity (critical   info   major   minor   warning);
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Select the severity that matches the lethality of the attack object on your network.
<b>Options</b>	<p>You can set the severity level to the following levels:</p> <ul style="list-style-type: none"><li>• <b>critical</b>—Contains attack objects matching exploits that attempt to evade detection, cause a network device to crash, or gain system-level privileges.</li><li>• <b>info</b>—Contains attack objects matching normal, harmless traffic containing URLs, DNS lookup failures, SNMP public community strings, and Peer-to-Peer (P2P) parameters. You can use informational attack objects to obtain information about your network.</li><li>• <b>major</b>—Contains attack objects matching exploits that attempt to disrupt a service, gain user-level access to a network device, or activate a Trojan horse previously loaded on a device.</li><li>• <b>minor</b>—Contains attack objects matching exploits that detect reconnaissance efforts attempting to access vital information through directory traversal or information leaks.</li><li>• <b>warning</b>—Contains attack objects matching exploits that attempt to obtain noncritical information or scan a network with a scanning tool.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## severity (Security IDP Dynamic Attack Group)

---

<b>Syntax</b>	severity { values [critical info major minor warning]; }
<b>Hierarchy Level</b>	[edit security idp dynamic-attack-group <i>dynamic-attack-group-name</i> filters]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a severity filter to add attack objects based on the attack severity levels.
<b>Options</b>	<p><b>values</b>—Name of the severity filter. You can select from the following severity:</p> <ul style="list-style-type: none"><li>• <b>critical</b>—The attack is a critical one.</li><li>• <b>info</b>—Provide information of attack when it matches.</li><li>• <b>major</b>—The attack is a major one.</li><li>• <b>minor</b>—The attack is a minor one.</li><li>• <b>warning</b>—Issue a warning when attack matches.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## severity (Security IDP IPS Rulebase)

---

<b>Syntax</b>	severity (critical   info   major   minor   warning);
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set the rule severity levels in logging to support better organization and presentation of log records on the log server. You can use the default severity settings of the selected attack object, or choose a specific severity for your rule. The severity you configure in the rules overrides the inherited attack severity.
<b>Options</b>	<p>You can set the severity level to the following levels:</p> <ul style="list-style-type: none"><li>• <b>critical</b>—2</li><li>• <b>info</b>—3</li><li>• <b>major</b>—4</li><li>• <b>minor</b>—5</li><li>• <b>warning</b>—7</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## shellcode

---

<b>Syntax</b>	shellcode (all   intel   no-shellcode   sparc);
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type anomaly] [edit security idp custom-attack <i>attack-name</i> attack-type signature]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Shellcode signifies that the attack is a shellcode attack and is capable of creating its own shell.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>all</b>—All shellcode checks will be performed if this attack matches.</li> <li>• <b>intel</b>—Basic shellcode checks and Intel-specific shellcode checks will be performed.</li> <li>• <b>no-shellcode</b>—No shellcode checks will be performed.</li> <li>• <b>sparc</b>—Basic shellcode checks and Sparc-specific shellcode checks will be performed.</li> </ul> <p><b>Default:</b> Basic shellcode checks will be performed when this field is not configured.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## signature (Security IDP)

---

**Syntax**    `signature {`  
              `context context-name;`  
              `direction (any | client-to-server | server-to-client);`  
              `negate;`  
              `pattern signature-pattern;`  
              `protocol {`  
                  `icmp {`  
                      `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 {`  
                  `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;`  
                  `}`  
                  `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;
  }
  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;
  }
  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;
}
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 {
    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;
}
nested-application nested-application-name;
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);
}

```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** IDP uses stateful signatures to detect attacks. Stateful signatures are more specific than regular signatures. With stateful signatures, IDP can look for the specific protocol or service used to perpetrate the attack.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## source (Security IDP IP Headers)

---

<b>Syntax</b>	<pre>source {     match (equal   greater-than   less-than   not-equal);     value <i>ip-address-or-hostname</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the IP address or hostname of the attacking device.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>ip-address-or-hostname</i>—Match an IP address or a hostname.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## source-address (Security IDP Policy)

<b>Syntax</b>	source-address ([ <i>address-name</i> ]   any   any-ipv4   any-ipv6);
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a source IP address or IP address set object to be used as the match source address object. The default value is any.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b><i>address-name</i></b>—IP address or IP address set object.</li> <li>• <b><i>any</i></b>—Specify any IPv4 or IPv6 address.</li> <li>• <b><i>any-ipv4</i></b>—Specify any IPv4 address.</li> <li>• <b><i>any-ipv6</i></b>—Specify any IPv6 address.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## source-address (Security IDP Sensor Configuration)

<b>Syntax</b>	source-address <i>ip-address</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the source IP address for the carrier UDP packet.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## source-except

---

<b>Syntax</b>	<code>source-except [<i>address-name</i>];</code>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-exempt rule <i>rule-name</i> match] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a source IP address or IP address set object to specify all source address objects except the specified address objects. The default value is any.
<b>Options</b>	<b><i>address-name</i></b> —IP address or IP address set object.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## source-port (Security IDP)

---

<b>Syntax</b>	<code>source-port {     match (equal   greater-than   less-than   not-equal);     value <i>source-port</i>; }</code>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol udp] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the port number on the attacking device.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match (equal   greater-than   less-than   not-equal)</b>—Match an operand.</li><li>• <b>value <i>source-port</i></b>—Port number on the attacking device.</li></ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## ssl-inspection

---

<b>Syntax</b>	<pre>ssl-inspection {   cache-prune-chunk-size <i>number</i>;   key-protection;   maximum-cache-size <i>number</i>;   session-id-cache-timeout <i>seconds</i>;   sessions <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Inspect HTTP traffic encrypted in SSL protocol. SSL inspection is disabled by default. It is enabled if you configure SSL inspection.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> <li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li> </ul>

## start-log

---

<b>Syntax</b>	start-log <i>value</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log suppression]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify how many instances of a specific event must occur before log suppression begins.
<b>Options</b>	<i>value</i> —Log suppression begins after how many occurrences. <b>Range:</b> 1 through 128 <b>Default:</b> 1
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## start-time (Security IDP)

---

<b>Syntax</b>	<code>start-time <i>start-time</i>;</code>
<b>Hierarchy Level</b>	[edit security idp security-package automatic]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the time that the device automatically starts downloading the updated signature database from the specified URL.
<b>Options</b>	<i>start-time</i> —Time in MM-DD.hh:mm format.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## statistics (Security IDP)

---

<b>Syntax</b>	<pre>statistics {     interval <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration application-ddos]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	The <b>statistics</b> option enables application-level DDoS statistic collection at the defined interval. Statistic report files are stored on the routing engine data storage device in /var/log/addos in comma separated value (CSV) format. The data storage device must have at least 2 GB of free space before logging will occur.
<b>Options</b>	<b>interval <i>minutes</i></b> —Set the interval in minutes that will define when application statistic will be collected. <b>Range:</b> 1 through 60 minutes (1-minute increments) <b>Default:</b> 1 minute
<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>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>



## suppression

---

<b>Syntax</b>	<pre> suppression {   disable;   (include-destination-address   no-include-destination-address);   max-logs-operate <i>value</i>;   max-time-report <i>value</i>;   start-log <i>value</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration log]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Log suppression reduces the number of logs by displaying a single record for multiple occurrences of the same event. Log suppression can negatively impact sensor performance if the reporting interval is set too high. By default this feature is enabled.
<b>Options</b>	<p><b>disable</b>—Disable log suppression.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p><b>security</b>—To view this statement in the configuration.</p> <p><b>security-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## target (Security IDP)

---

<b>Syntax</b>	target (destination-address   service   source-address   source-zone   source-zone-address   zone-service);
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the blocking options that you want to set to block the future connections. Blocking options can be based on the following matches of the attack traffic:
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>destination-address</b>—Matches traffic based on the destination address of the attack traffic.</li><li>• <b>service</b>—For TCP and UDP, matches traffic based on the source address, source port, destination address, and destination port of the attack traffic. This is the default.  For ICMP flows, the destination port is 0. Any ICMP flow matching source port, source address, and destination address is blocked.</li><li>• <b>source-address</b>—Matches traffic based on the source address of the attack traffic.</li><li>• <b>source-zone</b>—Matches traffic based on the source zone of the attack traffic.</li><li>• <b>source-zone-address</b>—Matches traffic based on the source zone and source address of the attack traffic.</li><li>• <b>zone-service</b>—Matches traffic based on the source zone, destination address, destination port, and protocol of the attack traffic.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

---

## tcp (Security IDP Protocol Binding)

---

<b>Syntax</b>	tcp { minimum-port <i>port-number</i> <maximum-port <i>port-number</i> >; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Allow IDP to match the attack for specified TCP ports.
<b>Options</b>	<b>minimum-port <i>port-number</i></b> —Minimum port in the port range. <b>Range:</b> 0 through 65,535  <b>maximum-port <i>port-number</i></b> —Maximum port in the port range. <b>Range:</b> 0 through 65,535
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## tcp (Security IDP Signature Attack)

```

Syntax  tcp {
        ack-number {
            match (equal | greater-than | less-than | not-equal);
            value acknowledgement-number;
        }
        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;
        }
        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;
    }
}
```

<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the TCP header information for the signature attack.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## tcp-flags

<b>Syntax</b>	<pre> 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); } </pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify that IDP looks for a pattern match whether or not the TCP flag is set.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>ack   no-ack</b>—When set, the acknowledgment flag acknowledges receipt of a packet.</li> <li>• <b>fin   no-fin</b>—When set, the final flag indicates that the packet transfer is complete and the connection can be closed.</li> <li>• <b>psh   no-psh</b>—When set, the push flag indicates that the receiver should push all data in the current sequence to the destination application (identified by the port number) without waiting for the remaining packets in the sequence.</li> <li>• <b>r1   no-r1</b>—When set, indicates that the R1 retransmission threshold has been reached.</li> <li>• <b>r2   no-r2</b>—When set, indicates that the R2 retransmission threshold has been reached.</li> <li>• <b>rst   no-rst</b>—When set, the reset flag resets the TCP connection, discarding all packets in an existing sequence.</li> <li>• <b>syn   no-syn</b>—When set, indicates that the sending device is asking for a three-way handshake to initialize communications.</li> <li>• <b>urg   no-urg</b>—When set, the urgent flag indicates that the packet data is urgent.</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## terminal

---

<b>Syntax</b>	terminal;
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set or unset a terminal rule flag. The device stops matching rules for a session when a terminal rule is matched.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## test (Security IDP)

---

<b>Syntax</b>	test <i>test-condition</i> ;
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type anomaly]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify protocol anomaly condition to be checked.
<b>Options</b>	<i>test-condition</i> —Name of the anomaly test condition.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## then (Security IDP Policy)

```
Syntax  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);
    }
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.

**Description** Specify the action to be performed when traffic matches the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*
- *IDP Class of Service Action Feature Guide for Security Devices*



## then (Security Rulebase DDos)

```
Syntax  then {
        action {
            (close-server | drop-connection | drop-packet | no-action);
        }
        ip-action {
            (ip-block | ip-close | ip-connection-rate-limit connections-per-second | ip-notify);
            log;
            log-create;
            refresh-timeout;
            timeout seconds;
        }
        notification {
            log-attacks {
                alert;
            }
        }
    }
```

**Hierarchy Level** [edit security idp idp-policy *policy-name* rulebase-ddos rule *rule-name*]

**Release Information** Statement introduced in Junos OS Release 10.0.

**Description** Specify the session action to be performed when traffic matches the defined criteria.

**Options** The remaining statements are explained separately.

**Required Privilege Level** security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- *Application-Level Distributed Denial of Service Feature Guide for Security Devices*
- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## time-binding

---

<b>Syntax</b>	<pre>time-binding {     count <i>count-value</i>;     scope (destination   peer   source); }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to detect a sequence of the same attacks over a period of time.
<b>Options</b>	The remaining statements are explained separately.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## timeout (Security IDP Policy)

---

<b>Syntax</b>	<pre>timeout <i>seconds</i>;</pre>
<b>Hierarchy Level</b>	[edit security idp idp-policy <i>policy-name</i> rulebase-ddos rule <i>rule-name</i> then ip-action] [edit security idp idp-policy <i>policy-name</i> rulebase-ips rule <i>rule-name</i> then ip-action]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the number of seconds that you want the IP action to remain in effect after a traffic match.
<b>Options</b>	<b>seconds</b> —Number of seconds the IP action should remain effective. <b>Range:</b> 0 through 64,800 seconds <b>Default:</b> 0 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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## to-zone (Security IDP Policy)

<b>Syntax</b>	<code>to-zone (zone-name   any);</code>
<b>Hierarchy Level</b>	<code>[edit security idp idp-policy policy-name rulebase-ddos rule rule-name match]</code> <code>[edit security idp idp-policy policy-name rulebase-exempt rule rule-name match]</code> <code>[edit security idp idp-policy policy-name rulebase-ips rule rule-name match]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for <b>rulebase-ddos</b> introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a destination zone to be associated with the security policy. The default value is any.
<b>Options</b>	<b>zone-name</b> —Name of the destination zone object.
<b>Required Privilege Level</b>	<b>security</b> —To view this statement in the configuration. <b>security-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## tos

---

<b>Syntax</b>	<pre>tos {     match (equal   greater-than   less-than   not-equal);     value <i>type-of-service-in-decimal</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the type of service.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value <i>type-of-service-in-decimal</i></b>—The following service types are available:<ul style="list-style-type: none"><li>• 0000—Default</li><li>• 0001—Minimize Cost</li><li>• 0002—Maximize Reliability</li><li>• 0003—Maximize Throughput</li><li>• 0004—Minimize Delay</li><li>• 0005—Maximize Security</li></ul></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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## total-length

<b>Syntax</b>	total-length { match (equal   greater-than   less-than   not-equal); value <i>total-length-of-ip-datagram</i> ; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the number of bytes in the packet, including all header fields and the data payload.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li>• <b>value</b> <i>total-length-of-ip-datagram</i>—Length of the IP datagram.</li> </ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## total-memory

<b>Syntax</b>	total-memory <i>percentage</i> ;
<b>Hierarchy Level</b>	[edit security idp sensor-configuration packet-log]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the maximum amount of memory to be allocated to packet capture for the device. This value is expressed as a percentage of the memory available on the device. The total memory for a device will differ depending on its operating mode.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>percentage</b>—Amount of packet capture memory expressed as a percentage of total memory for the device mode.</li> </ul> <p><b>Range:</b> 1 to 100 percent <b>Default:</b> 10</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>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## traceoptions (Security Datapath Debug)

```
Syntax  traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        no-remote-trace;
    }
```

**Hierarchy Level** [edit security datapath-debug]

**Release Information** Command introduced in Junos OS Release 9.6.

**Description** Sets the trace options for datapath-debug.

**Options** • **file**—Configure the trace file options.

- **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.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

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). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the 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 file size, you also must specify a maximum number of trace files with the files 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
- **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**    • *IDP Monitoring and Troubleshooting Guide for Security Devices*

## traceoptions (Security IDP)

<b>Syntax</b>	<pre> traceoptions {   file {     filename;     files number;     match regular-expression;     size maximum-file-size;     (world-readable   no-world-readable);   }   flag all;   level (all   error   info   notice   verbose   warning);   no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit security idp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure IDP 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 <b>trace-file.0</b> again reaches its maximum size, <b>trace-file.1</b> is renamed <b>trace-file.2</b> and <b>trace-file.0</b> is renamed <b>trace-file.1</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.
  - **all**—Trace with all flags enabled
- **level**—Set the level of debugging the output option.
  - **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**—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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li></ul>
------------------------------	--

## ttl (Security IDP)

---

<b>Syntax</b>	<pre>ttl {     match (equal   greater-than   less-than   not-equal);     value <i>time-to-live</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol ipv4]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the time-to-live (TTL) value of the packet. This value represents the number of routers the packet can pass through. Each router that processes the packet decrements the TTL by 1; when the TTL reaches 0, the packet is discarded.
<b>Options</b>	<p><b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</p> <p><b>value <i>time-to-live</i></b>—The time-to-live value.</p> <p><b>Range:</b> 0 through 255</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## tunable-name

---

<b>Syntax</b>	<code>tunable-name <i>tunable-name</i> {     tunable-value <i>protocol-value</i>; }</code>
<b>Hierarchy Level</b>	[edit security idp sensor-configuration detector protocol-name <i>protocol-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for file format decoding over HTTP using MIME added in Junos OS Release 11.2.
<b>Description</b>	Specify the name of the tunable parameter to enable or disable the protocol detector for each of the service. By default, the protocol decoders for all services are enabled.
<b>Options</b>	<p><i>tunable-name</i>—Name of the specific tunable parameter.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li></ul>

## tunable-value

---

<b>Syntax</b>	<code>tunable-value protocol-value;</code>
<b>Hierarchy Level</b>	<code>[edit security idp sensor-configuration detector protocol-name protocol-name tunable-name tunable-name]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. Support for file format decoding over HTTP using MIME added in Junos OS Release 11.2.
<b>Description</b>	Specify the value of the tunable parameter to enable or disable the protocol detector for each of the services.
<b>Options</b>	<i>tunable-value</i> —Integer representing a selected option for the switch specified in <i>tunable-name</i> . The range of values depends on the options defined for the specified switch.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP SSL Inspection Feature Guide for Security Devices</i></li></ul>

## type (Security IDP Dynamic Attack Group)

---

<b>Syntax</b>	<pre>type {   values [anomaly signature]; }</pre>
<b>Hierarchy Level</b>	<code>[edit security idp dynamic-attack-group dynamic-attack-group-name filters]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify an attack type filter to add attack objects based on the type of attack object (signature or protocol anomaly).
<b>Options</b>	<i>values</i> —Name of the attack type filter.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## type (Security IDP ICMP Headers)

---

<b>Syntax</b>	<pre>type {     match (equal   greater-than   less-than   not-equal);     value <i>type-value</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol icmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the primary code that identifies the function of the request/reply.
<b>Options</b>	<p><b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</p> <p><b>value <i>type-value</i></b>—Match a decimal value.</p> <p><b>Range:</b> 0 through 255</p>
<b>Required Privilege Level</b>	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## udp (Security IDP Protocol Binding)

---

<b>Syntax</b>	udp { minimum-port <i>port-number</i> <maximum-port <i>port-number</i> >; }
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type chain protocol-binding] [edit security idp custom-attack <i>attack-name</i> attack-type signature protocol-binding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Allow IDP to match the attack for specified UDP ports.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>minimum-port <i>port-number</i></b>—Minimum port in the port range. <b>Range:</b> 0 through 65,535</li><li>• <b>maximum-port <i>port-number</i></b>—Maximum port in the port range. <b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## udp (Security IDP Signature Attack)

```
Syntax  udp {
          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;
          }
        }
```

**Hierarchy Level** [edit security idp custom-attack *attack-name* attack-type signature protocol]

**Release Information** Statement introduced in Junos OS Release 9.3.

**Description** Allow IDP to match the UDP header information for the signature attack.

**Options** The remaining statements are explained separately.

**Required Privilege** security—To view this statement in the configuration.  
**Level** security-control—To add this statement to the configuration.

**Related Documentation**

- *IDP Policies Feature Guide for Security Devices*
- *IDP Application Identification Feature Guide for Security Devices*

## urgent-pointer

---

<b>Syntax</b>	<pre>urgent-pointer {   match (equal   greater-than   less-than   not-equal);   value <i>urgent-pointer</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the data in the packet is urgent; the URG flag must be set to activate this field.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>urgent-pointer</i>—Match the value of the urgent pointer.</li></ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## url (Security IDP)

---

<b>Syntax</b>	<pre>url <i>url-name</i>;</pre>
<b>Hierarchy Level</b>	[edit security idp security-package]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the URL to automatically download the updated signature database.
<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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li></ul>



## window-scale

---

<b>Syntax</b>	<pre> window-scale {     match (equal   greater-than   less-than   not-equal);     value <i>window-scale-factor</i>; } </pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the scale factor that the session of the attack will use. The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header.
<b>Options</b>	<ul style="list-style-type: none"> <li><b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li> <li><b>value</b> <i>window-scale-factor</i>—Match the number of bytes.</li> </ul> <p><b>Range:</b> 0 through 255</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><i>IDP Policies Feature Guide for Security Devices</i></li> <li><i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>

## window-size

---

<b>Syntax</b>	<pre>window-size {     match (equal   greater-than   less-than   not-equal);     value <i>window-size</i>; }</pre>
<b>Hierarchy Level</b>	[edit security idp custom-attack <i>attack-name</i> attack-type signature protocol tcp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the number of bytes in the TCP window size.
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>match</b> (equal   greater-than   less-than   not-equal)—Match an operand.</li><li>• <b>value</b> <i>window-size</i>—Match the number of bytes.</li></ul> <p><b>Range:</b> 0 through 65,535</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>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>

## Administration

---

- [Alarms and Auditing on page 2176](#)
- [Packet Capture on page 2177](#)
- [Tuning on page 2182](#)
- [Clear Commands on page 2183](#)
- [Request Commands on page 2198](#)
- [Show Commands on page 2208](#)

## Alarms and Auditing

- [IDP Alarms and Auditing on page 2176](#)

### IDP Alarms and Auditing

---

By default, IDP logs the occurrence of an event without raising an alarm to the administrator. When the system is configured to log an event and the **potential-violation** option is set, IDP logs on the Packet Forwarding Engine are forwarded to Routing Engine. The Routing Engine then parses the IDP attack logs and raises IDP alarms as necessary.

- To enable an IDP alarm, use the **set security alarms potential-violation idp** command.
- To verify that the configuration is working properly, use the **show security alarms** command.



**NOTE:** In releases before Junos OS Release 11.2, IDP attack logs contain information about an attack event but do not raise alarms to the administrator.

#### Related Documentation

- [IDP Policies Overview](#)
- [Understanding IDP Log Information Usage on the IC Series UAC Appliance on page 1997](#)

## Packet Capture

- [Example: Configuring Security Packet Capture on page 2177](#)
- [Example: Configuring Packet Capture for Datapath Debugging on page 2179](#)
- [Verifying Security Packet Capture on page 2182](#)

### Example: Configuring Security Packet Capture

This example shows how to configure the security packet capture.

- [Requirements on page 2177](#)
- [Overview on page 2177](#)
- [Configuration on page 2177](#)
- [Verification on page 2179](#)

#### Requirements

Before you begin, configure network interfaces.

#### Overview

In this example, you configure a packet capture for rule 1 of policy pol0. The rule specifies that, if an attack occurs, 10 packets before the attack and 3 packets after the attack will be captured, and that the post-attack capture should time out after 60 seconds. The sensor configuration is modified to allocate 5 percent of available memory and 15 percent of the IDP sessions to packet capture. When the packet capture object is prepared, it is transmitted from device 10.56.97.3 to port 5 on device 10.24.45.7.

#### 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 security idp idp-policy pol0 rulebase-ips rule 1 then notification packet-log pre-attack
  10 post-attack 3 post-attack-timeout 60
set security idp sensor-configuration packet-log total-memory 5 max-sessions 15
  source-address 10.56.97.3 host 10.24.45.7 port 5
```

**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 the security packet capture:

1. Navigate to the notification level for rule 1, policy pol0 in the configuration hierarchy.

```
[edit]
user@host# edit security idp idp-policy pol0 rulebase-ips rule 1 then notification
```

2. Define the size and timing constraints for each packet capture.

```
[edit security idp idp-policy pol0 rulebase-ips rule 1 then notification]
user@host# set packet-log pre-attack 10 post-attack 3 post-attack-timeout 60
```

3. Enable the security idp sensor-configuration.

```
[edit]
user@host# edit security idp sensor-configuration
```

4. Allocate the device resources to be used for packet capture.

```
[edit security idp sensor-configuration]
user@host# set packet-log total-memory 5 max-sessions 15
```

5. Identify the source and host devices for transmitting the packet-capture object.

```
[edit security idp sensor-configuration]
user@host# set packet-log source-address 10.56.97.3 host 10.24.45.7 port 5
```

**Results** From configuration mode, confirm your configuration by entering the **show security idp** 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 idp

idp-policy pol0 {
  rulebase-ips {
    rule 1 {
      then {
        notification {
          packet-log {
            pre-attack 10;
            post-attack 3;
            post-attack-timeout 60;
          }
        }
      }
    }
  }
  sensor-configuration {
    packet-log {
      host 10.24.45.7 5;
      max-sessions 15;
      source-address 10.56.97.3;
      total-memory 5;
    }
  }
}
```

```
}
}
```

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

### Verification

Confirm that the configuration is working properly.

- [Verifying Security Packet Capture on page 2179](#)

### Verifying Security Packet Capture

**Purpose** Verify security packet capture.

**Action** From operational mode, enter the **show security idp counters packet-log** command.

```
user@host> show security idp counters packet-log
```

IDP counters:	Value
Total packets captured since packet capture was activated	0
Total sessions enabled since packet capture was activated	0
Sessions currently enabled for packet capture	0
Packets currently captured for enabled sessions	0
Packet clone failures	0
Session log object failures	0
Session packet log object failures	0
Sessions skipped because session limit exceeded	0
Packets skipped because total memory limit exceeded	0

**Related Documentation** • [Understanding Security Packet Capture on page 1998](#)

### 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 2179](#)
- [Overview on page 2179](#)
- [Configuration on page 2180](#)
- [Verification on page 2181](#)

### Requirements

Before you begin, see “[Debugging the Data Path \(CLI Procedure\)](#)” on page 1279.

### 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.

```
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*.

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 2181](#)
- [Verifying data path debugging capture on page 2182](#)
- [Verifying data path debugging counter on page 2182](#)

### 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
```

**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 1246](#)
  - [Understanding Data Path Debugging for SRX Series Devices on page 1242](#)
  - [Debugging the Data Path \(CLI Procedure\) on page 1279](#)

**Verifying Security Packet Capture**

**Purpose** Monitor packet capture statistics issuing the following `show` command from the CLI prompt.

**Action** `user@host> show security idp counters packet-log`

IDP counters:	Value
Total packets captured since packet capture was activated	0
Total sessions enabled since packet capture was activated	0
Sessions currently enabled for packet capture	0
Packets currently captured for enabled sessions	0
Packet clone failures	0
Session log object failures	0
Session packet log object failures	0
Sessions skipped because session limit exceeded	0
Packets skipped because total memory limit exceeded	0

- Related Documentation**
- [Understanding Security Packet Capture on page 1998](#)
  - [Example: Configuring Security Packet Capture on page 2177](#)
  - [Example: Configuring Packet Capture for Datapath Debugging on page 1289](#)

**Tuning**

- [Configuring Session Capacity for IDP \(CLI Procedure\) on page 2182](#)

**Configuring Session Capacity for IDP (CLI Procedure)**

The configuration instructions in this topic describe how modify session capacity for IDP policies.

You do this by adding the `maximize-idp-sessions` command and then adding the weight option to specify IDP sessions.





**NOTE:** The weight option depends on the `maximize-idp-sessions` command being set.

1. If you have an active IDP policy, you can configure the device to increase IDP session capacity by entering following command:  

```
user@host#set security forwarding-process application-services maximize-idp-sessions
```
2. You can further adjust the weight of the firewall and IDP processing functions, such as in the case of heavier IDP policies with the following command:..  

```
user@host#set security forwarding-process application-services maximize-idp-sessions weight idp
```
3. Commit your changes. You must reboot the device for any session capacity setting changes to take effect.



**NOTE:** If the device has `maximize-idp-sessions` weight enabled for IDP, and you do not have an IDP policy configured, a warning message appears when you commit your configuration. If you see this warning, you should remove your configured settings.

To turn `maximize-idp-sessions` settings off, remove the `maximize-idp-sessions` configuration.



**NOTE:** You must reboot the device for any `maximize-idp-sessions` setting changes to take effect.

#### Related Documentation

- [IDP Policies Overview](#)
- [Performance and Capacity Tuning for IDP Overview on page 1998](#)

## Clear Commands

- `clear security datapath-debug counters`
- `clear security idp`
- `clear security idp application-ddos cache`
- `clear security idp attack table`
- `clear security idp counters application-identification`
- `clear security idp counters dfa`
- `clear security idp counters flow`
- `clear security idp counters http-decoder`
- `clear security idp counters ips`
- `clear security idp counters log`

- `clear security idp counters packet`
- `clear security idp counters policy-manager`
- `clear security idp counters tcp-reassembler`
- `clear security idp ssl-inspection session-id-cache`

## clear security datapath-debug counters

---

<b>Syntax</b>	clear security datapath-debug counters
<b>Release Information</b>	Command introduced in Junos OS Release 10.0.
<b>Description</b>	Clear all data path-debugging counters.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security datapath-debug capture on page 1596</a></li><li>• <a href="#">show security datapath-debug counter on page 1597</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear security datapath-debug counters on page 2185</a>
<b>Output Fields</b>	This command produces no output.

### Sample Output

#### clear security datapath-debug counters

```
user@host> clear security datapath-debug counters
```

## clear security idp

---

<b>Syntax</b>	clear security idp (application-identification   application-statistics   attack   counters   status)
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Clear the following IDP information:</p> <ul style="list-style-type: none"><li>• <b>application-identification</b>—Clear IDP application identification data.</li><li>• <b>application-statistics</b>—Clear IDP application statistics.</li><li>• <b>attack</b>—Clear IDP attack data</li><li>• <b>counters</b>—Clear IDP counters</li><li>• <b>status</b>—Clear IDP Status</li></ul>
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">clear security idp status on page 2186</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### clear security idp status

```
user@host> clear security idp status
State of IDP: 2-default, Up since: 2010-02-04 13:37:16 UTC (17:13:45 ago)

Packets/second: 0 Peak: 0 @ 2010-02-05 06:49:51 UTC
KBits/second: 0 Peak: 0 @ 2010-02-05 06:49:51 UTC
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 @ 2010-02-05 06:49:51 UTC]
TCP: [Current: 0] [Max: 0 @ 2010-02-05 06:49:51 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: 0] [UDP: 0] [Other: 0]
Policy Name: sample
Running Detector Version: 10.4.160091104
```

## clear security idp application-ddos cache

---

<b>Syntax</b>	clear security idp application-ddos cache
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Clear application-level distributed denial-of-service (DDOS) state including context, context value, and client classification.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp application-ddos application on page 2215</a></li><li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp attack table

---

<b>Syntax</b>	clear security idp attack table
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Clear details of the IDP attack table.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp attack table on page 2220</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters application-identification

---

<b>Syntax</b>	clear security idp counters application-identification
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the application identification counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">application-identification on page 2026</a></li><li>• <a href="#">show security idp counters application-identification on page 2224</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters dfa

---

<b>Syntax</b>	clear security idp counters dfa
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the DFA counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp counters dfa on page 2226</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.



## clear security idp counters flow

---

<b>Syntax</b>	clear security idp counters flow
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the IDP flow-related counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">flow (Security IDP) on page 2068</a></li><li>• <a href="#">show security idp counters flow on page 2227</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters http-decoder

---

<b>Syntax</b>	clear security idp counters http-decoder
<b>Release Information</b>	Command introduced in Junos OS Release 11.2.
<b>Description</b>	Reset all the HTTP decoder counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp counters http-decoder on page 2234</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters ips

---

<b>Syntax</b>	clear security idp counters ips
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the ips counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">ips on page 2088</a></li><li>• <a href="#">show security idp counters ips on page 2235</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters log

---

<b>Syntax</b>	clear security idp counters log
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the IDP log counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">event-rate on page 1672</a></li><li>• <a href="#">show security idp counters log on page 2238</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters packet

---

<b>Syntax</b>	clear security idp counters packet
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the IDP packet counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp counters packet on page 2241</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## [clear security idp counters policy-manager](#)

---

<b>Syntax</b>	clear security idp counters policy-manager
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the IDP policies counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp counters policy-manager on page 2246</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp counters tcp-reassembler

---

<b>Syntax</b>	clear security idp counters tcp-reassembler
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Reset all the TCP reassembler counter values.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">re-assembler on page 2118</a></li><li>• <a href="#">show security idp counters tcp-reassembler on page 2247</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.

## clear security idp ssl-inspection session-id-cache

---

<b>Syntax</b>	clear security idp ssl-inspection session-id-cache
<b>Release Information</b>	Command introduced in Junos OS Release 9.3.
<b>Description</b>	Clear all the entries stored in the SSL session ID cache.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp ssl-inspection session-id-cache on page 2261</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">clear security idp ssl-inspection session-id-cache on page 2198</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### clear security idp ssl-inspection session-id-cache

```
user@host> clear security idp ssl-inspection session-id-cache
Total SSL session cache entries cleared : 2
```

### Request Commands

- [request security datapath-debug capture start](#)
- [request security idp security-package download](#)
- [request security idp security-package install](#)
- [request security idp ssl-inspection key add](#)
- [request security idp ssl-inspection key delete](#)
- [request security idp storage-cleanup](#)



## request security datapath-debug capture start

---

<b>Syntax</b>	request security datapath-debug capture start
<b>Release Information</b>	Command introduced in Junos OS Release 10.0.
<b>Description</b>	Start the data path debugging capture.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request security datapath-debug capture start

```
user@host> request security datapath-debug capture start
datapath-debug capture started on file
```

## request security idp security-package download

<b>Syntax</b>	<pre>request security idp security-package download &lt;check-server&gt; &lt;full-update&gt; &lt;policy-templates&gt; &lt;version <i>version-number</i> &gt; &lt;status&gt;</pre>
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. Detailed status added in Junos OS Release 10.1. Description modified in Junos OS Release 11.1. Application package support added in Junos OS Release 11.4.
<b>Description</b>	<p>Manually download the individual components of the security package from the Juniper Security Engineering portal. The components are downloaded into a staging folder inside the device.</p> <p>By default, this command tries to download the delta set attack signature table. It also downloads IDP, IPS, and application package signatures.</p>
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>check-server</b>—(Optional) Retrieve the version information of the latest security package from the security portal server.</li> <li>• <b>full-update</b>—(Optional) Download the latest security package with the full set of attack signature tables from the portal.</li> <li>• <b>policy-templates</b>—(Optional) Download the latest policy templates from the portal.</li> <li>• <b>version <i>version-number</i></b>—(Optional) Download the security package of a specific version from the portal.</li> <li>• <b>status</b>—(Optional) Provide detailed status of security package download operation.</li> </ul>
<b>Additional Information</b>	The <b>request security idp security-package download</b> command does not download security package files if the installed version on the device is same as the security package version on the server ( <a href="https://services.netscreen.com/cgi-bin/index.cgi">https://services.netscreen.com/cgi-bin/index.cgi</a> always). The <b>request security idp security-package download full-update</b> command downloads the latest security package files on the device from the server, irrespective of the version on the device and the server.
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li> <li>• <a href="#">show security idp active-policy on page 99</a></li> <li>• <a href="#">show security idp security-package-version on page 2258</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">request security idp security-package download on page 2201</a>

[request security idp security-package download policy-templates on page 2201](#)  
[request security idp security-package download version 1151 full-update on page 2201](#)  
[request security idp security-package download status on page 2201](#)

**Output Fields** When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request security idp security-package download

```
user@host> request security idp security-package download
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1152(Thu Apr 24 14:37:44 2008, Detector=9.1.140080400)
```

## Sample Output

### request security idp security-package download policy-templates

```
user@host> request security idp security-package download policy-templates
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:35
```

## Sample Output

### request security idp security-package download version 1151 full-update

```
user@host> request security idp security-package download version 1151 full-update
Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1151(Wed Apr 23 14:39:15 2008, Detector=9.1.140080400)
```

### request security idp security-package download status

To request status for a package download:

```
user@host> request security idp security-package download status
Done;Successfully downloaded
from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2014(Thu Oct 20 12:07:01 2011, Detector=11.6.140110920)
```

To request status for a template download:

```
user@host> request security idp security-package download status
Done; Successfully downloaded from
(https://services.netscreen.com/cgi-bin/index.cgi).
```

When devices are operating in chassis cluster mode, when you check the security package download status, a message is displayed confirming that the downloaded security package is being synchronized to the primary and secondary nodes.

```
user@host> request security idp security-package download status
node0:
-----
Done;Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi)
and synchronized to backup.
Version info:2011(Mon Oct 17 15:13:06 2011, Detector=11.6.140110920)
```

## request security idp security-package install

---

<b>Syntax</b>	<code>request security idp security-package install</code> <code>&lt;policy-templates&gt;</code> <code>&lt;status&gt;</code> <code>&lt;update-attack-database-only&gt;</code>
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. Description modified in Junos OS Release 11.1. Added application package support in Junos OS Release 11.4.
<b>Description</b>	<p>Updates the attack database inside the device with the newly downloaded one from the staging folder, recompiles the existing running policy, and pushes the recompiled policy to the data plane.</p> <p>Also, if there is an existing running policy, and the previously installed detector's version is different from the newly downloaded one, the downloaded components are pushed to the data plane. This command installs IDP, IPS, and application package signatures.</p>
<b>Options</b>	<ul style="list-style-type: none"><li>• <b>policy-templates</b>—(Optional) Installs the policy template file into <code>/var/db/scripts/commit/templates</code>.</li><li>• <b>status</b>—(Optional) The command <b>security-package install</b> may take a long time depending on the new Security database size. Hence, <b>security-package install</b> command returns immediately and a background process performs the task. User can check the status using <b>security-package install status</b> command.</li><li>• <b>update-attack-database-only</b>—(Optional) Loads the security package into IDP database but does not compile/push the active policy or the new detector to the data plane.</li></ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li><li>• <a href="#">show security idp active-policy on page 99</a></li><li>• <a href="#">show security idp security-package-version on page 2258</a></li></ul>
<b>List of Sample Output</b>	<a href="#">request security idp security-package install on page 2202</a> <a href="#">request security idp security-package install status on page 2203</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

### request security idp security-package install

```
user@host> request security idp security-package install
Will be processed in async mode. Check the status using the status checking CLI
```

## Sample Output

### request security idp security-package install status

To request status on a package installation:

```
user@host> request security idp security-package install status
Done; Attack DB update : successful - [UpdateNumber=1152, ExportDate=Thu Apr 24
14:37:44 2008]
    Updating data-plane with new attack or detector : not performed
    due to no existing active policy found.
```

To request status on a template installation:

```
user@host> request security idp security-package install status
Done; policy-template has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xml)!
```

## request security idp ssl-inspection key add

<b>Syntax</b>	<code>request security idp ssl-inspection key add &lt;key-name&gt; [file &lt;file-name&gt;] [password &lt;password-string&gt;] [server &lt;server-ip&gt;]</code>
<b>Release Information</b>	Command introduced in Junos OS Release 9.3.
<b>Description</b>	Install a Privacy-Enhanced Mail (PEM) key that is optionally password protection, and associate a server with an installed key. The length of each key name and password string should not exceed 32 alphanumeric characters.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>key-name</b>—Name of the SSL private key.</li> <li>• <b>file &lt;file-name&gt;</b>—(Optional) Location of RSA private key (PEM format) file.</li> <li>• <b>password &lt;password-string&gt;</b>—(Optional) Password used to encrypt specified key.</li> <li>• <b>server &lt;server-ip&gt;</b>—(Optional) Server IP address to be added to the specified key.</li> </ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show security idp ssl-inspection key on page 2259</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted on page 2204</a> <a href="#">request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted on page 2204</a> <a href="#">request security idp ssl-inspection key add key3 file /var/tmp/norm.key on page 2205</a> <a href="#">request security idp ssl-inspection key add key1 server 1.1.0.1 on page 2205</a> <a href="#">request security idp ssl-inspection key add key1 server 1.1.0.2 on page 2205</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

[request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted](#)

```
user@host> request security idp ssl-inspection key add key1 file /var/tmp/enc1.key password encrypted
Added key 'key1'
```

### Sample Output

[request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted](#)

```
user@host> request security idp ssl-inspection key add key2 file /var/tmp/enc2.key password encrypted
Added key 'key2', server 2.2.0.1
```

### Sample Output

request security idp ssl-inspection key add key3 file /var/tmp/norm.key

```
user@host> request security idp ssl-inspection key add key3 file /var/tmp/norm.key
Added key 'key3'
```

### Sample Output

request security idp ssl-inspection key add key1 server 1.1.0.1


```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.1
Added key 'key1', server 1.1.0.1
```

### Sample Output

request security idp ssl-inspection key add key1 server 1.1.0.2

```
user@host> request security idp ssl-inspection key add key1 server 1.1.0.2
Added key 'key1', server 1.1.0.2
```

## request security idp ssl-inspection key delete

<b>Syntax</b>	request security idp ssl-inspection key delete [ <b>&lt;key-name&gt;</b> ] [ <b>server &lt;server-ip&gt;</b> ]
<b>Release Information</b>	Command introduced in Junos OS Release 9.3.
<b>Description</b>	Delete the specified server IP from the given key if the server is specified. If the server IP is not specified, the given key will be deleted along with all the server addresses associated with it.
<div>  <b>NOTE:</b> You will get a delete confirmation question before deleting one or more keys or server. </div>	
<b>Options</b>	<ul style="list-style-type: none"> <li><b>key-name</b>—(Optional) Name of the SSL private key.</li> <li><b>server &lt;server-ip&gt;</b> —(Optional) Server IP address associated with the specified key to be deleted.</li> </ul>
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">show security idp ssl-inspection key on page 2259</a></li> <li><i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">request security idp ssl-inspection key delete on page 2206</a> <a href="#">request security idp ssl-inspection key delete key1 on page 2206</a> <a href="#">request security idp ssl-inspection key delete key2 server 2.2.0.1 on page 2207</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request security idp ssl-inspection key delete

```
user@host> request security idp ssl-inspection key delete
```

```
This command will delete one or more ssl keys.  
Continue? [yes,no] (no) yes
```

```
Number of keys 4, server 3 deleted
```

### Sample Output

#### request security idp ssl-inspection key delete key1

```
user@host> request security idp ssl-inspection key delete key1
```

```
This command will delete one or more ssl keys.  
Continue? [yes,no] (no) yes
```



Number of keys 1, server 2 deleted

## Sample Output

`request security idp ssl-inspection key delete key2 server 2.2.0.1`

```
user@host> request security idp ssl-inspection key delete key2 server 2.2.0.1
```

This command will delete one or more ssl keys.

Continue? [yes,no] (no) yes

Number of keys 0, server 1 deleted

## request security idp storage-cleanup

---

<b>Syntax</b>	request security idp storage-cleanup
<b>Release Information</b>	Command introduced in Junos OS Release 11.4.
<b>Description</b>	Delete unused files to free up storage space on a device.
<b>Options</b>	<b>cache-files</b> — Delete DFA cache files used for optimizing idp policy compilation.  <b>downloaded-files</b> — Delete downloaded security-package files (with out affecting the installed database).
<b>Required Privilege Level</b>	maintenance
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>List of Sample Output</b>	<a href="#">request security idp storage-cleanup on page 2208</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

#### request security idp storage-cleanup

```
user@host> request security idp storage-cleanup downloaded-files
Successfully deleted downloaded secdb files
```

### Show Commands

- [show security flow session idp family](#)
- [show security flow session idp summary](#)
- [show security idp active-policy](#)
- [show security idp application-ddos application](#)
- [show security idp attack description](#)
- [show security idp attack detail](#)
- [show security idp attack table](#)
- [show security idp counters application-ddos](#)
- [show security idp counters application-identification](#)
- [show security idp counters dfa](#)
- [show security idp counters flow](#)
- [show security idp counters http-decoder](#)
- [show security idp counters ips](#)
- [show security idp counters log](#)

- `show security idp counters packet`
- `show security idp counters packet-log`
- `show security idp counters policy-manager`
- `show security idp counters tcp-reassembler`
- `show security idp logical-system policy-association`
- `show security idp memory`
- `show security idp policies`
- `show security idp policy-commit-status`
- `show security idp policy-commit-status clear`
- `show security idp policy-templates`
- `show security idp predefined-attacks`
- `show security idp security-package-version`
- `show security idp ssl-inspection key`
- `show security idp ssl-inspection session-id-cache`
- `show security idp status`
- `show security idp status detail`

## show security flow session idp family

<b>Syntax</b>	show security flow session idp family (inet   inet6)
<b>Release Information</b>	Command introduced in Junos OS Release 10.2. Support for family inet6 added in Junos OS Release 12.1X46-D10.
<b>Description</b>	Display filtered summary of information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions.
<b>Options</b>	inet—Display details summary of IPv4 sessions.  inet6—Display details summary of IPv6 sessions.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Monitoring and Troubleshooting Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security flow session summary family inet on page 2210</a> <a href="#">show security flow session summary family inet6 on page 2211</a>
<b>Output Fields</b>	Table 279 on page 2210 lists the output fields for the <b>show security flow session summary family</b> command. Output fields are listed in the approximate order in which they appear.

Table 279: show security flow session summary Output Fields

Field Name	Field Description
Valid sessions	Count of valid sessions.
Pending sessions	Count of pending sessions.
Invalidated sessions	Count of sessions the security device has determined to be invalid.
Sessions in other states	Count of sessions not in valid, pending, or invalidated state.
Total sessions	Total of the above counts.

## Sample Output

### show security flow session summary family inet

```

user@host> show security flow session summary family inet
Flow Sessions on FPC4 PIC0:
Valid sessions: 3
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 3

Flow Sessions on FPC5 PIC0:

```

```
Valid sessions: 4  
Pending sessions: 0  
Invalidated sessions: 0  
Sessions in other states: 0  
Total sessions: 4
```

#### `show security flow session summary family inet6`

```
user@host> show security flow session summary family inet6
```

```
Flow Sessions on FPC1 PIC1:  
Valid sessions: 20  
Pending sessions: 0  
Invalidated sessions: 0  
Sessions in other states: 0  
Total sessions: 20
```

## show security flow session idp summary

<b>Syntax</b>	<b>show security flow session idp summary</b>
<b>Release Information</b>	Command introduced in Junos OS Release 10.2.
<b>Description</b>	Display summary output.
<b>Options</b>	<ul style="list-style-type: none"> <li>• application—Application name</li> <li>• destination-port—Destination port</li> <li>• destination-prefix—Destination IP prefix or address</li> <li>• family—Display session by family.</li> <li>• interface—Name of incoming or outgoing interface</li> <li>• protocol—IP protocol number</li> <li>• source-port—Source port</li> <li>• source-prefix—Source IP prefix</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show security flow session on page 102</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security flow session idp summary on page 2213</a>
<b>Output Fields</b>	<a href="#">Table 280 on page 2212</a> lists the output fields for the <b>show security flow session idp summary</b> command. Output fields are listed in the approximate order in which they appear.

**Table 280: show security flow session idp summary Output Fields**

Field Name	Field Description
Valid session	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalid sessions.
Sessions in other states	Number of sessions in other states.
Total sessions	Total number of sessions.

## Sample Output

### show security flow session idp summary

```
root@ show security flow session idp summary
```

```
Flow Sessions on FPC4 PIC0:
```

```
Valid sessions: 3
```

```
Pending sessions: 0
```

```
Invalidated sessions: 0
```

```
Sessions in other states: 0
```

```
Total sessions: 3
```

```
Flow Sessions on FPC5 PIC0:
```

```
Valid sessions: 4
```

```
Pending sessions: 0
```

```
Invalidated sessions: 0
```

```
Sessions in other states: 0
```

```
Total sessions: 4
```

## show security idp active-policy

<b>Syntax</b>	show security idp active-policy
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display information about the policy name and running detector version with which the policy is compiled from the IDP data plane module.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">request security idp security-package download on page 2200</a></li> <li>• <a href="#">request security idp security-package install on page 2202</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Class of Service Action Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp active-policy on page 2214</a>
<b>Output Fields</b>	Table 12 on page 99 lists the output fields for the <b>show security idp active-policy</b> command. Output fields are listed in the approximate order in which they appear.

Table 281: 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 application-ddos application

<b>Syntax</b>	show security idp application-ddos application
<b>Release Information</b>	Command introduced in Junos OS Release 10.0.
<b>Description</b>	Display basic statistics for the servers being protected by the IDP application-level DDoS feature.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>application-name</b>—Display information on a specific application-level DDoS application profile.</li> <li>• <b>context</b>—Name of the application context for <i>application-name</i></li> <li>• <b>detail</b>—Display a detailed view of the protected servers.</li> <li>• <b>server</b>—IP address of protected server.</li> <li>• <b>zone</b>—Zone name where the protected server resides.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp application-ddos application on page 2216</a> <a href="#">show security idp application-ddos application detail on page 2216</a>
<b>Output Fields</b>	<a href="#">Table 282 on page 2215</a> lists the output fields for the <b>show security idp application-ddos application</b> command.

**Table 282: show security idp application-ddos Output Fields**

Field Name	Field Description
Zone	Security zone where the protected server resides.
Server	IP address of the protected server.
Application	Name of the application-level DDoS application.
Conn/sec	Number of client connections to the protected server.
Context	Protocol context that is being monitored.
Contexts/tick	Number of protocol context hits measured per tick. One tick equals 60 seconds by default.

## Sample Output

### show security idp application-ddos application

```
user@host> show security idp application-ddos application
```

Zone	Server	Application	Conn/sec	Context	Contexts/tick
trust	81.0.3.1	http-server-1	2648/sec	http-header-user-agent	35746/60sec
trust	81.1.0.2	dns-server-1	4517/sec	dns-type-name	263234/60sec
trust	81.1.0.2	dns-server-1	1497/sec	dns-type-name	88061/60sec
trust	81.0.3.1	http-server1	1496/sec	http-url-parsed	81177/60sec

...

## Sample Output

### show security idp application-ddos application detail

```
user@host> show security idp application-ddos application detail
```

```
Zone: trust Server: 81.1.0.2 Application: dns-server-1 Connections/sec:
1499/secContext: dns-type-name Contexts/tick: 88061/60sec
Value: 00 05 74 65 73 74 6e 61 6d 65 2e 6a 75 6e 69 70 testname.juniper.net
Value: 65 72 2e 6e 65 74
Context values/tick : 29143/60sec
```

```
Zone: trust Server: 81.0.3.1 Application: http-server-1 Connections/sec:
2615/secContext: http-url contexts/tick: 148196/60sec
Value: 2f 6e 65 74 73 63 72 65 65 6e 2e 68 746d 6c /netscreen.htm
Context values/tick : 26809/60sec
```

...

## show security idp attack description

Syntax	<code>show security idp attack description <i>attack-name</i></code>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Display description of a specified IDP attack.
Options	<ul style="list-style-type: none"> <li><i>attack-name</i> —IDP attack name.</li> </ul>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <li><a href="#">clear security idp attack table on page 2188</a></li> <li><i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
List of Sample Output	<a href="#">show security idp attack description on page 2217</a>
Output Fields	<a href="#">Table 283 on page 2217</a> lists the output fields for the <code>show security idp attack description</code> command. Output fields are listed in the approximate order in which they appear.

Table 283: show security idp attack description Output Fields

Field Name	Field Description
Description	IDP attack description.

## Sample Output

### show security idp attack description

```
user@host> show security idp attack description FTP:USER:ROOT
```

Description: This signature detects attempts to login to an FTP server using the "root" account. This can indicate an attacker trying to gain root-level access, or it can indicate poor security practices. FTP typically uses plain-text passwords, and using the root account to FTP could expose sensitive data over the network.

## show security idp attack detail

<b>Syntax</b>	<b>show security idp attack detail <i>attack-name</i></b>
<b>Release Information</b>	Command introduced in Junos OS Release 11.4.
<b>Description</b>	Display details of a specified IDP attack.
<b>Options</b>	<ul style="list-style-type: none"> <li><b><i>attack-name</i></b> —IDP attack name.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">clear security idp attack table on page 2188</a></li> <li><i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp attack detail on page 2218</a>
<b>Output Fields</b>	<a href="#">Table 284 on page 2218</a> lists the output fields for the <b>show security idp attack detail</b> command. Output fields are listed in the approximate order in which they appear.

**Table 284: show security idp attack detail Output Fields**

Field Name	Field Description
Display Name	Display name of the IDP attack.
Severity	Severity level of the IDP attack.
Category	IDP attack category.
Recommended	Specifies whether a default action for the IDP attack is recommended by Juniper Networks (true or false).
Recommended Action	Recommended action for the IDP attack.
Type	Type of IDP attack.
Direction	Direction of the IDP attack.
False Positives	Specifies whether the IDP attack produces false positive on the network.
Service	IDP service configured for the IDP attack. If a service is configured for the IDP attack, the IDP service name is displayed. Otherwise, <b>Not available</b> is displayed.

## Sample Output

### show security idp attack detail

```
user@host> show security idp attack detail FTP:USER:ROOT
```

Display Name: FTP: "root" Account Login  
Severity: Minor  
Category: FTP  
Recommended: false  
Recommended Action: None  
Type: signature  
Direction: CTS  
False Positives: unknown  
Service: Not available

## show security idp attack table

<b>Syntax</b>	show security idp attack table
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display detailed information of IDP attack table.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp attack table on page 2188</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp attack table on page 2220</a>
<b>Output Fields</b>	Table 285 on page 2220 lists the output fields for the <b>show security idp attack table</b> command. Output fields are listed in the approximate order in which they appear.

**Table 285: show security idp attack table Output Fields**

Field Name	Field Description
<b>Attack name</b>	Name of the attack that you want to match in the monitored network traffic.
<b>Hits</b>	<p>Total number of attack matches.</p> <p>On SRX Series and J Series devices, for brute force and time-binding-related attacks, the logging is to be done only when the match <b>count</b> is equal to the <b>threshold</b>. That is, only one log is generated within the 60-second period in which the threshold is measured. This process prevents repetitive logs from being generated and ensures consistency with other IDP platforms, such as IDP-standalone.</p> <p>When no attack is seen within the 60-second period and the BFQ entry is flushed out, the match count starts over the new attack match shows up in the attack table, and the log is generated.</p>

## Sample Output

### show security idp attack table

```

user@host> show security idp attack table
IDP attack statistics:
  Attack name                               #Hits
  HTTP:OVERFLOW:PI3WEB-SLASH-OF             1

```

## show security idp counters application-ddos

<b>Syntax</b>	show security idp counters application-ddos
<b>Release Information</b>	Command introduced in Junos OS Release 10.0.
<b>Description</b>	Display the status of all IDP application-ddos counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Application-Level Distributed Denial of Service Feature Guide for Security Devices</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters application-ddos on page 2222</a>
<b>Output Fields</b>	Table 286 on page 2221 lists the output fields for the <b>show security idp counters application-ddos</b> command. Output fields are listed in the approximate order in which they appear.

**Table 286: show security idp counters application-ddos Output Fields**

Field Name	Field Description
App-DDOS inspected flows	Number of client-to-server flows inspected for application-ddos.
App-DDOS failed flows	Number of client-to-server flows that failed during application-ddos processing.
App-DDOS ignored flows	Number of client-to-server flows ignored for application-ddos.
App-DDOS first path failed	Number of client-to-server flow initialization failures during first path.
App-DDOS first path succeeded	Number of successful client-to-server flow initialization during first path.
App-DDOS dropped packets	Number of packets dropped in the application-level DDoS module.
App-DDOS processed packets	Number of total packets processed in the application-level DDoS module.
App-DDOS connection table process succeeded	Number of times connection processing succeeded.
App-DDOS connection table process failed	Number of times connection processing failed.
App-DDOS context process succeeded	Number of times the context processing succeeded.
App-DDOS context process failed	Number of times context processing failed.
App-DDOS ignore context	Number of contexts ignored if the flow is not client-to-server or if the application-level DDoS module is disabled.

Table 286: show security idp counters application-ddos Output Fields (*continued*)

Field Name	Field Description
App-DDOS context values excluded	Number of context values excluded for actions, reporting, or both.
App-DDOS context value process succeeded	Number of times context value processing succeeded, including action and logging events if configured.
App-DDOS context value process failed	Number of times context value processing failed, including action and logging events if configured.
App-DDOS context value prune failed	Number of times context value pruning failed.
App-DDOS no action	Number of times an attack is detected and no action is taken.
App-DDOS drop connection action	Number of times an attack is detected and a drop connection action is taken.
App-DDOS drop packet action	Number of times an attack is detected and a drop packet action is taken.
App-DDOS close server action	Number of times an attack is detected and a close server action is taken.
App-DDOS IP Action block	Number of times an ip-action block entry is created and installed.
App-DDOS IP Action close	Number of times an ip-action close entry is created and installed.
App-DDOS Action notify	Number of times an ip-action notify entry is created and installed.
App-DDOS logs sent	Number of attack logs sent.
App-DDOS logs report failed	Number of attack log reports that failed.

## Sample Output

### show security idp counters application-ddos

```
user@host> show security idp counters application-ddos
```

```

App-DDOS inspected flows          447172
App-DDOS failed flows             0
App-DDOS ignored flows            12267
App-DDOS first path failed        0
App-DDOS first path succeeded     459439
App-DDOS dropped packets          0
App-DDOS processed packets        449118
App-DDOS connection table process succeeded 459439
App-DDOS connection table process failed 0
App-DDOS context process succeeded 449118
App-DDOS context process failed 0
App-DDOS ignore context           0
App-DDOS context values excluded 0
App-DDOS context value process succeeded 449118
App-DDOS context value process failed 0
App-DDOS context value prune failed 0

```



App-DDOS no action	275996
App-DDOS drop connection action	0
App-DDOS drop packet action	0
App-DDOS close server action	0
App-DDOS IP Action block	0
App-DDOS IP Action close	0
App-DDOS IP Action notify	275996
App-DDOS logs sent	238
App-DDOS logs report failed	0

## show security idp counters application-identification

<b>Syntax</b>	show security idp counters application-identification
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. Modified in Junos OS Release 12.1.
<b>Description</b>	Display the status of all IDP application identification (AI) counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp counters application-identification on page 2189</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters application-identification on page 2225</a>
<b>Output Fields</b>	<a href="#">Table 287 on page 2224</a> lists the output fields for the <b>show security idp counters application-identification</b> command. Output fields are listed in the approximate order in which they appear.

**Table 287: show security idp counters application-identification Output Fields**

Field Name	Field Description
AI matches	Number of sessions with an AI signature match.
AI no-matches	Number of sessions with no AI signature match.
AI-enabled sessions	Number of sessions with AI enabled.
AI-disabled sessions	Number of sessions with AI disabled.
AI-disabled sessions due to ssl encapsulated flows	Number of sessions with AI disabled due to SSL encapsulated flows.
AI-disabled sessions due to cache hit	Number of sessions with AI disabled due to a cache match.
AI-disabled sessions due to configuration	Number of sessions with AI disabled because the configured session limit was reached.
AI-disabled sessions due to protocol remapping	Number of sessions with AI disabled due to protocol remapping.
AI-disabled sessions due to RPC match	Number of sessions with AI disabled due to an RPC match.
AI-disabled sessions due to non-TCP/UDP flows	Number of sessions with AI disabled due to non-TCP or non-UDP flows.

Table 287: show security idp counters application-identification Output Fields (*continued*)

Field Name	Field Description
AI-disabled sessions due to session limit	Number of sessions with AI disabled because the maximum session limit was reached.
AI-disabled sessions due to session packet memory limit	Number of sessions with AI disabled because the memory usage limit per session was reached.
AI-disabled sessions due to global packet memory limit	Number of sessions with AI disabled because the global memory usage limit was reached.
Packets cloned for AI	Number of packets cloned for application identification.
Policy update	Number of times the IDP policy has been updated.

## Sample Output

### show security idp counters application-identification

```

user@host> show security idp counters application-identification
IDP counters:
IDP counter type                                Value
AI matches                                       4
AI no-matches                                   0
AI-enabled sessions                             4
AI-disabled sessions                            0
AI-disabled sessions due to gate match           0
AI-disabled sessions due to ssl encapsulated flows 0
AI-disabled sessions due to cache hit            0
AI-disabled sessions due to configuration        0
AI-disabled sessions due to protocol remapping   0
AI-disabled sessions due to RPC match            0
AI-disabled sessions due to non-TCP/UDP flows    0
AI-disabled sessions due to session limit        0
AI-disabled sessions due to session packet memory limit 0
AI-disabled sessions due to global packet memory limit 0
Packets cloned for AI                           12
Policy update                                   0

```

## show security idp counters dfa

<b>Syntax</b>	show security idp counters dfa
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display the status of all DFA counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp counters dfa on page 2190</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters dfa on page 2226</a>
<b>Output Fields</b>	<a href="#">Table 288 on page 2226</a> lists the output fields for the <b>show security idp counters dfa</b> command. Output fields are listed in the approximate order in which they appear.

**Table 288: show security idp counters dfa Output Fields**

Field Name	Field Description
DFA Group Merged Usage	Number of DFA groups merged.
DFA Matches	Number of DFA matches found.

## Sample Output

### show security idp counters dfa

```

user@host> show security idp counters dfa
IDP counters:
IDP counter type
DFA Group Merged Usage      Value
DFA Matches                  0
                             1

```

## show security idp counters flow

<b>Syntax</b>	show security idp counters flow
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display the status of all IDP flow counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">flow (Security IDP) on page 2068</a></li> <li>• <a href="#">clear security idp counters flow on page 2191</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters flow on page 2231</a>
<b>Output Fields</b>	<a href="#">Table 289 on page 2227</a> lists the output fields for the <b>show security idp counters flow</b> command. Output fields are listed in the approximate order in which they appear.

**Table 289: show security idp counters flow Output Fields**

Field Name	Description
Fast-path packets	Number of packets that are set through fast path after completing IDP policy lookup.
Slow-path packets	Number of packets that are sent through slow path during IDP policy lookup.
Session construction failed (Unsupported)	Number of times the packet failed to establish the session.
Session limit reached	Number of sessions that reached IDP sessions limit.
Session inspection depth reached	Number of sessions that reached inspection depth.
Memory limit reached	Number of sessions that reached memory limit.
Not a new session (Unsupported)	Number of sessions that extended beyond time limit.
Invalid index at age-out (Unsupported)	Invalid session index in session age-out message.
Packet logging	Number of packets saved for packet logging.
Policy cache hits	Number of sessions that matched policy cache.
Policy cache misses	Number of sessions that did not match policy cache.

Table 289: show security idp counters flow Output Fields (*continued*)

Field Name	Description
Policy cache entries	Number of policy cache entries.
Maximum flow hash collisions	Maximum number of packets, of one flow, that share the same hash value.
Flow hash collisions	Number of packets that share the same hash value.
Gates added	Number of gate entries added for dynamic port identification.
Gate matches (Unsupported)	Number of times a gate is matched.
Sessions deleted	Number of sessions deleted.
Sessions aged-out (Unsupported)	Number of sessions that are aged out if no traffic is received within session timeout value.
Sessions in-use while aged-out (Unsupported)	Number of sessions in use during session age-out.
TCP flows marked dead on RST/FIN	Number of sessions marked dead on TCP RST/FIN.
policy init failed	Policy initiation failed.
Number of times Sessions exceed high mark	Number of times sessions exceeded the high mark.
Number of sessions exceeds high mark	Number of sessions that exceed high mark.
Number of sessions drops below low mark	Number of sessions that fall below low mark.
Memory of sessions exceeds high mark	Session memory exceeds high mark.
Memory of sessions drops below low mark	Session memory drops below low mark.
SM Sessions encountered memory failures	Number of SM sessions that encountered memory failures.
SM Packets on sessions with memory failures	Number of SM packets that encountered memory failures.
Sessions constructed	Number of sessions established.

Table 289: show security idp counters flow Output Fields (*continued*)

Field Name	Description
SM Sessions dropped	Number of SM sessions dropped.
SM sessions ignored	Number of sessions ignored in Security Module (SM).
SM sessions interested	Number of SM sessions interested.
SM sessions not interested	Number of SM sessions not interested.
SM sessions interest error	Number of errors created for SM sessions interested.
Sessions destructed	Number of sessions destructed.
SM Session Create	Number of SM sessions created.
SM Packet Process	Number of packets processed from SM.
SM FTP data session ignored by IDP	Number of SM FTP data sessions that are ignored by IDP.
SM Session close	Number of SM sessions closed.
SM client-to-server packets	Number of SM client-to-server packets.
SM server-to-client packets	Number of SM server-to-client packets.
SM client-to-server L7 bytes	Number of SM client-to-server Layer 7 bytes.
SM server-to-client L7 bytes	Number of SM server-to-client Layer 7 bytes.
Client-to-server flows ignored	Number of client-to-server flow sessions that are ignored.
Server-to-client flows ignored	Number of server-to-client flow sessions that are ignored.
Server-to-client flows tcp optimized	Number of server-to-client flow TCP sessions that are optimized
Client-to-server flows tcp optimized	Number of client-to-server flow TCP sessions that are optimized
Both directions flows ignored	Number of server-to-client and client-to-server flow sessions that are ignored.
Fail-over sessions dropped	Number of failover sessions dropped.
Sessions dropped due to no policy	Number of sessions dropped because there was no active IDP policy.
IDP Stream Sessions dropped due to memory failure	Number of IDP stream sessions that are dropped because of memory failure.
IDP Stream Sessions ignored due to memory failure	Number of IDP stream sessions that are ignored because of memory failure.

Table 289: show security idp counters flow Output Fields (*continued*)

Field Name	Description
<b>IDP Stream Sessions closed due to memory failure</b>	Number of IDP stream sessions that are closed because of memory failure.
<b>IDP Stream Sessions accepted</b>	Number of IDP stream sessions that are accepted.
<b>IDP Stream Sessions constructed</b>	Number of IDP stream sessions that are constructed.
<b>IDP Stream Sessions destructed</b>	Number of IDP stream sessions that are destructed.
<b>IDP Stream Move Data</b>	Number of Stream data events handled by IDP.
<b>IDP Stream Sessions ignored on JSF SSL Event</b>	Number of IDP stream sessions that are ignored because of a JSF SSL proxy event.
<b>IDP Stream Sessions not processed for no matching rules</b>	Number of IDP stream sessions that are not processed for no matching rules.
<b>IDP Stream stbuf dropped</b>	Number of IDP stream plugin buffers dropped.
<b>IDP Stream stbuf reinjected</b>	Number of IDP stream plugin buffers injected.
<b>Busy packets from stream plugin</b>	Number of packets saved as one or more packets of this session from stream plugin.
<b>Busy packets from packets plugin</b>	Number of saved packets for IDP stream plugin sessions.
<b>Bad kpp</b>	Number of internal marked packets logged for IDP processing.
<b>Lsys policy id lookup failed sessions</b>	Number of sessions that failed logical systems policy lookup
<b>Busy packets</b>	Number of packets saved as one or more packets of this session are handed off for asynchronous processing.
<b>Busy packet errors</b>	Number of packets found with IP checksum error after asynchronous processing is completed.
<b>Dropped queued packets (async mode)</b>	Number of queued packets dropped based on policy action, reinjection failures, or if the session is marked to destruct.
<b>Dropped queued packets failed (async mode)</b>	Not used currently.
<b>Reinjected packets (async mode)</b>	Number of packets reinjected into the queue.
<b>Reinjected packets failed (async mode)</b>	Number of failed reinjected packets.
<b>AI saved processed packet</b>	Number of AI packets saved for which the asynchronous processing is completed.



Table 289: show security idp counters flow Output Fields (*continued*)

Field Name	Description
<b>Busy packet count incremented</b>	Number of times the busy packet count incremented in asynchronous processing.
<b>busy packet count decremented</b>	Number of times the busy packet count decremented in asynchronous processing.
<b>session destructed in pme</b>	Number of sessions destructed as a part of asynchronous result processing.
<b>session destruct set in pme</b>	Number of sessions set to be destructed as a result of asynchronous processing.
<b>KQ op</b>	Number of sessions with one of the following status: <ul style="list-style-type: none"> <li>• KQ op hold—number of times packets held by IDP.</li> <li>• KQ op drop—number of times packets dropped by IDP.</li> <li>• KQ op route—number of times IDP decided to be route the packet directly.</li> <li>• KQ op Continue—number of times IDP decided to continue to process the packet.</li> <li>• KQ op error—number of times error occurred while IPD processing packet.</li> <li>• KQ op stop—number of times IDP decided to stop processing the packet.</li> </ul>
<b>PME wait not set</b>	Number of AI saved packets given for signature matching.
<b>PME wait set</b>	Number of packets given for signature matching without AI save.
<b>PME KQ run not called</b>	Number of times signature matching results processed out of packet receiving order.

## Sample Output

### show security idp counters flow

```
user@host> show security idp counters flow
IDP counters:
```

IDP counter type	Value
Fast-path packets	40252
Slow-path packets	127
Session construction failed	0
Session limit reached	0
Session inspection depth reached	0
Memory limit reached	0
Not a new session	0
Invalid index at ageout	0
Packet logging	0
Policy cache hits	92
Policy cache misses	67
Policy cache entries	67
Maximum flow hash collisions	0
Flow hash collisions	0
Gates added	0
Gate matches	0
Sessions deleted	127
Sessions aged-out	0
Sessions in-use while aged-out	0
TCP flows marked dead on RST/FIN	13

Policy init failed	0
Number of times Sessions exceed high mark	0
Number of times Sessions drop below low mark	0
Memory of Sessions exceeds high mark	0
Memory of Sessions drops below low mark	0
SM Sessions encountered memory failures	0
SM Packets on sessions with memory failures	0
IDP session gate creation requests	0
IDP session gate creation acknowledgements	0
IDP session gate hits	0
IDP session gate timeouts	0
Number of times Sessions crossed the CPU threshold value that is set	0
Number of times Sessions crossed the CPU upper threshold	0
Sessions constructed	127
SM Sessions ignored	0
SM Sessions dropped	0
SM Sessions interested	168
SM Sessions not interested	4
SM Sessions interest error	0
Sessions destructed	127
SM Session Create	127
SM Packet Process	52257
SM ftp data session ignored by idp	0
SM Session close	127
SM Client-to-server packets	20066
SM Server-to-client packets	32191
SM Client-to-server L7 bytes	167292
SM Server-to-client L7 bytes	28523514
Client-to-server flows ignored	1
Server-to-client flows ignored	1
Server-to-client flows tcp optimized	3
Client-to-server flows tcp optimized	0
Both directions flows ignored	32
Fail-over sessions dropped	0
Sessions dropped due to no policy	0
IDP Stream Sessions dropped due to memory failure	0
IDP Stream Sessions ignored due to memory failure	0
IDP Stream Sessions closed due to memory failure	0
IDP Stream Sessions accepted	0
IDP Stream Sessions constructed	0
IDP Stream Sessions destructed	0
IDP Stream Move Data	0
IDP Stream Sessions ignored on JSF SSL Event	0
IDP Stream Sessions not processed for no matching rules	0
IDP Stream stbuf dropped	0
IDP Stream stbuf reinjected	0
Busy pkts from stream plugin	0
Busy pkts from pkt plugin	0
bad kpp	0
Lsys policy id lookup failed sessions	0
Busy packets	0
Busy packet Errors	0
Dropped queued packets (async mode)	0
Dropped queued packets failed(async mode)	0
Reinjected packets (async mode)	0
Reinjected packets failed(async mode)	0
AI saved processed packet	0
busy packet count incremented	0
busy packet count decremented	0
session destructed in pme	0

session destruct set in pme	0
kq op hold	0
kq op drop	0
kq op route	0
kq op continue	35155
kq op error	0
kq op stop	0
PME wait not set	0
PME wait set	0
PME KQ run not called	0

## show security idp counters http-decoder

<b>Syntax</b>	show security idp counters http-decoder
<b>Release Information</b>	Command introduced in Junos OS Release 11.2.
<b>Description</b>	Display the status of all HTTP decoders.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp counters http-decoder on page 2192</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters http-decoder on page 2234</a>
<b>Output Fields</b>	Table 290 on page 2234 lists the output fields for the <b>show security idp counters http-decoder</b> command. Output fields are listed in the approximate order in which they appear.

**Table 290: show security idp counters http-decoder Output Fields**

Field Name	Field Description
No of file-decoder requests from MIME over HTTP	Number of active file decoder requests sent over HTTP from MIME.
No of pending file-decoder requests from MIME over HTTP	Number of pending file decoder requests sent over HTTP from MIME.
No of completed file-decoder requests from MIME over HTTP	Number of completed file decoder requests sent over HTTP from MIME.
No of unrecognized file type from MIME over HTTP	Number of unrecognized file types sent over HTTP from MIME.
No of compressed payload transferred over HTTP	Number of compressed files transferred over HTTP from MIME.

## Sample Output

### show security idp counters http-decoder

```

user@host> show security idp counters http-decoder
IDP counters:
IDP counter type                                     Value
No of file-decoder requests from MIME over HTTP      0
No of pending file-decoder requests from MIME over HTTP 0
No of completed file-decoder requests from MIME over HTTP 0
No of unrecognized file type from MIME over HTTP      0
No of compressed payload transferred over HTTP        0

```

## show security idp counters ips

<b>Syntax</b>	show security idp counters ips
<b>Release Information</b>	Command modified in Junos OS Release 11.2.
<b>Description</b>	Display the status of all IPS counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">ips on page 2088</a></li> <li>• <a href="#">clear security idp counters ips on page 2193</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters ips on page 2236</a>
<b>Output Fields</b>	<p><a href="#">Table 291 on page 2235</a> lists the output fields for the <b>show security idp counters ips</b> command. Output fields are listed in the approximate order in which they appear.</p>

**Table 291: show security idp counters ips Output Fields**

Field Name	Field Description
TCP fast path	Number of TCP packets skipped for IDS processing.
Layer-4 anomalies	Number of Layer-4 protocol error or anomaly.
Anomaly hash misses	Number of times look failed on anomaly hash.
Line context matches	Number of attempts to match line based attacks in traffic stream.
Stream256 context matches	Number of attempts to match stream based attacks in first 256 bytes of traffic stream.
Stream context matches	Number of attempts to match stream based attacks in traffic stream.
Packet context matches	Number of attempts to match packet based attacks in traffic packet.
Packet header matches	Number of attempts to match packet header based attacks in traffic packet.
Context matches	Number of attempts to match protocol context based attacks in traffic stream.
Regular expression matches	Number of attempts to match PCRE expressions in traffic stream.
Tail DFAs	Number of attempts to match an attack on tail DFA group matches.
Exempted attacks	Number of attacks exempted from match as per exempt rulebase.
Out of order chains	Number of times attack is excluded from match due to member attacks in an attack group did not complete chain.

Table 291: show security idp counters ips Output Fields (*continued*)

Field Name	Field Description
Partial chain matches	Number of attacks in partial chain match with attack scope as transaction.
IDS device FIFO size	Number of IDS contexts in virtual IDS device.
IDS device FIFO overflows	Number of times an IDS context can not be written as the IDS device is full.
Brute force queue size	Number of entries in the brute force queue.
IDS cache hits (Unsupported)	Number of sessions those found attack instance in IDS cache.
IDS cache misses (Unsupported)	Number of sessions those did not find attack instance in IDS cache.
Shellcode detection invocations	Number of times shell code match is attempted.
Wrong offsets	Number of times attack's offset is not within the service offset range.
No peer MAC (Unsupported)	Number of times flow peer MAC address is not available.

## Sample Output

### show security idp counters ips

```

user@host> show security idp counters ips
IDP counters:
  IDP counter type                               Value
  TCP fast path                                  15
  Layer-4 anomalies                              0
  Anomaly hash misses                            3
  Line context matches                           5
  Stream256 context matches                      5
  Stream context matches                        5
  Packet context matches                        0
  Packet header matches                         0
  Context matches                               12
  Regular expression matches                     0
  Tail DFAs                                     0
  Exempted attacks                              0
  Out of order chains                           0
  Partial chain matches                         0
  IDS device FIFO size                          0
  IDS device FIFO overflows                     0
  Brute force queue size                        0
  IDS cache hits                                0
  IDS cache misses                              0
  Shellcode detection invocations                0
  Wrong offsets                                 0

```

No peer MAC	0
Content-decompression memory usage in KB	0
Content-decompression memory over limit	0
Content-decompression gunzip called	0
Content-decompression gunzip failed	0
Content-decompression others called	0
Content-decompression others failed	0
Content-decompression input bytes	0
Content-decompression output bytes	0
Content-decompression ratio over limit	0
Content-decompression type mismatch	0

## show security idp counters log

<b>Syntax</b>	show security idp counters log
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display the status of all IDP log counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">event-rate on page 1672</a></li> <li>• <i>clear security idp counters log</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters log on page 2240</a>
<b>Output Fields</b>	<a href="#">Table 292 on page 2238</a> lists the output fields for the <b>show security idp counters log</b> command. Output fields are listed in the approximate order in which they appear.

**Table 292: show security idp counters log Output Fields**

Field Name	Field Description
Logs dropped	Number of logs that are dropped.
Suppressed log count	Number of logs that are suppressed.
Logs waiting for post-window packets (Unsupported)	Number of logs waiting for post-window packets.
Logs ready to be sent (Unsupported)	Number of logs ready to be sent.
Logs in suppression list (Unsupported)	Number of logs considered for suppression list.
Log timers created	Number of times the log timer is created.
Log timers expired	Number of times the log timer is expired.
Log timers cancelled	Number of times the log timer is canceled.
Logs ready to be sent high watermark (Unsupported)	Number of packets that are ready to be sent with high degree watermark.



Table 292: show security idp counters log Output Fields (*continued*)

Field Name	Field Description
<b>Log receive buffer full</b> (Unsupported)	Number of times the buffer is full.
<b>Packet log too big</b> (Unsupported)	Number of packet logs that exceeded allowed packet log size.
<b>Reads per second</b> (Unsupported)	Number of packets that are read per second.
<b>Logs in read buffer high watermark</b> (Unsupported)	Number of high watermark packets that are in read buffer.
<b>Packets logged</b>	Number of packets that are logged,
<b>Packets lost</b> (Unsupported)	Number of packets that are failed to log.
<b>Packets copied</b> (Unsupported)	Number of packets copied during packet log.
<b>Packets held</b> (Unsupported)	Number of packets held for packet log.
<b>Packets released</b>	Number of packets that are released from hold.
<b>IP Action Messages</b> (Unsupported)	Number of IP action messages.
<b>IP Action Drops</b> (Unsupported)	Number of IP action messages dropped.
<b>IP Action Exists</b> (Unsupported)	Number of exits during IP action creation.
<b>NWaits</b> (Unsupported)	Number of logs waiting for post window packets.
<b>Match vectors</b>	Number of attacks in IDS match vector.
<b>Supercedes</b>	Number of attacks in supercede vector.

## Sample Output

### show security idp counters log

```
user@host> show security idp counters log
IDP counters:
IDP counter type                               Value
Logs dropped                                   0
Suppressed log count                           0
Logs waiting for post-window packets           0
Logs ready to be sent                          0
Logs in suppression list                       0
Log timers created                             0
Logs timers expired                            0
Log timers cancelled                           0
Logs ready to be sent high watermark            0
Log receive buffer full                        0
Packet log too big                             0
Reads per second                               1
Logs in read buffer high watermark              0
Log Bytes in read buffer high watermark         0
Packets logged                                 0
Packets lost                                   0
Packets copied                                 0
Packets held                                   0
Packets released                               0
IP Action Messages                             0
IP Action Drops                                0
IP Action Exists                               0
Nwaits                                          0
Match vectors                                  0
Supercedes                                     0
Kpacket too big                                0
```

## show security idp counters packet

<b>Syntax</b>	show security idp counters packet
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. The fields <b>Dropped by IDP policy</b> and <b>Dropped by Error</b> added in Junos OS Release 10.1.
<b>Description</b>	Display the status of all IDP packet counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp counters packet on page 2195</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters packet on page 2243</a>
<b>Output Fields</b>	Table 293 on page 2241 lists the output fields for the <b>show security idp counters packet</b> command. Output fields are listed in the approximate order in which they appear.

**Table 293: show security idp counters packet Output Fields**

Field Name	Field Description
Processed packets	Number of packets processed by the IDP service.
Dropped packets	Number of packets dropped by the IDP service.
Dropped by IDP policy	Number of packets dropped by the IDP policy.
Dropped by Error	Number of packets dropped by error.
Dropped sessions (Unsupported)	Number of sessions dropped.
Bad IP headers	Number of packets that fail IP header length validity check.
Packets with IP options	Number of packets that contain the optional header fields.
Decapsulated packets	Number of packets that are decapsulated.
GRE decapsulations (Unsupported)	Number of packets that are generic routing encapsulation (GRE) decapsulated.
PPP decapsulations (Unsupported)	Number of packets that are Point-to-Point Protocol (PPP) decapsulated.

Table 293: show security idp counters packet Output Fields (*continued*)

Field Name	Field Description
<b>GTP decapsulations</b> (Unsupported)	Number of packets that are GPRS tunneling protocol (GTP) decapsulated.
<b>GTP flows</b> (Unsupported)	Number of GTP flows.
<b>TCP decompression uncompressed IP</b> (Unsupported)	Number of uncompressed IP headers that are to be TCP decompressed.
<b>TCP decompression compressed IP</b> (Unsupported)	Number of compressed IP headers that are to be TCP decompressed.
<b>Deferred-send packets</b> (Unsupported)	Number of deferred IP packets that are sent out.
<b>IP-in-IP packets</b> (Unsupported)	Number of packets that are IP-in-IP encapsulated.
<b>TTL errors</b> (Unsupported)	Number of packets with TTL error in the header.
<b>Routing loops</b> (Unsupported)	Number of packets that continue to be routed in an endless circle due to an inconsistent routing state.
<b>No-route packets</b> (Unsupported)	Number of packets that could not be routed further.
<b>Flood IP</b> (Unsupported)	Number of packets that are identified as IP flood packets.
<b>Invalid ethernet headers</b> (Unsupported)	Number of packets that are identified with an invalid Ethernet header.
<b>Packets attached</b>	Number of packets attached.
<b>Packets cloned</b>	Number of packets that are cloned.
<b>Packets allocated</b>	Number of packets allocated.
<b>Packets destructed</b>	Number of packets destructed.

## Sample Output

### show security idp counters packet

```
user@host> show security idp counters packet
IDP counters:
IDP counter type                               Value
Processed packets                             27
Dropped packets                               0
Dropped by IDP policy                         0
Dropped by error                             0
Dropped sessions                             0
Bad IP headers                                0
Packets with IP options                       0
Decapsulated packets                          0
GRE decapsulations                           0
PPP decapsulations                           0
GTP decapsulations                           0
GTP flows                                    0
TCP decompression uncompressed IP             0
TCP decompression compressed IP              0
Deferred-send packets                         0
IP-in-IP packets                             0
TTL errors                                    0
Routing loops                                0
STP drops                                    0
No-route packets                             0
Flood IP                                     0
Invalid ethernet headers                     0
Packets attached                             28
Packets cloned                               28
Packets allocated                            0
Packets destructed                           55
```

## show security idp counters packet-log

**Syntax** show security idp counters packet-log

**Release Information** Command introduced in Junos OS Release 10.2.

**Description** Display the values of all IDP packet-log counters.

**Required Privilege Level** view

**Related Documentation** • *IDP Policies Feature Guide for Security Devices*

**Output Fields** The following table lists the output fields for the **show security idp counters packet-log** command. Output fields are listed in the approximate order in which they appear.

Field Name	Field Description
Total packets captured since packet capture was activated	Number of packets captured by the device by the IDP service.
Total sessions enabled since packet capture was activated	Number of sessions that have performed packet capture since the capture facility was activated.
Sessions currently enabled for packet capture	Number of sessions that are actively capturing packets at this time.
Packets currently captured for enabled sessions	Number of packets that have been captured by active sessions.
Packet clone failures	Number of packet capture failures due to cloning error.
Session log object failures	Number of objects containing log messages generated during packet capture that were not successfully transmitted to the host.
Session packet log object failures	Number of objects containing captured packets that were not successfully transmitted to the host.
Sessions skipped because session limit exceeded	Number of sessions that could not initiate packet capture because the maximum number of sessions specified for the device were conducting captures at that time.
Packets skipped because packet limit exceeded	Number of packets not captured because the packet limit specified for this device was reached.
Packets skipped because total memory limit exceeded	Number of packets not captured because the memory allocated for packet capture on this device was exceeded.

## Sample Output

### show security idp counters packet-log

```
user@host> show security idp counters packet-log
IDP counters:
Total packets captured since packet capture was activated      0
Total sessions enabled since packet capture was activated      0
Sessions currently enabled for packet capture                  0
Packets currently captured for enabled sessions                0
Packet clone failures                                         0
Session log object failures                                    0
Session packet log object failures                             0
Sessions skipped because session limit exceeded                0
Packets skipped because packet limit exceeded                  0
Packets skipped because total memory limit exceeded            0
```

## show security idp counters policy-manager

<b>Syntax</b>	show security idp counters policy-manager
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display the status of all IDP policies counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp counters policy-manager on page 2196</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters policy-manager on page 2246</a>
<b>Output Fields</b>	Table 294 on page 2246 lists the output fields for the <b>show security idp counters policy-manager</b> command. Output fields are listed in the approximate order in which they appear.

Table 294: show security idp counters policy-manager Output Fields

Field Name	Field Description
Number of policies	Number of policies installed.
Number of aged out policies	Number of IDP policies that are expired.

## Sample Output

### show security idp counters policy-manager

```

user@host> show security idp counters policy-manager
IDP counters:
  IDP counter type                Value
  Number of policies              0
  Number of aged out policies     0

```



## show security idp counters tcp-reassembler

<b>Syntax</b>	show security idp counters tcp-reassembler
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display the status of all TCP reassembler counter values.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">re-assembler on page 2118</a></li> <li>• <a href="#">clear security idp counters tcp-reassembler on page 2197</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp counters tcp-reassembler on page 2248</a>
<b>Output Fields</b>	<a href="#">Table 295 on page 2247</a> lists the output fields for the <b>show security idp counters tcp-reassembler</b> command. Output fields are listed in the approximate order in which they appear.

**Table 295: show security idp counters tcp-reassembler Output Fields**

Field Name	Field Description
Bad TCP checksums (Unsupported)	Number of packets that have incorrect TCP checksums.
Bad TCP headers	Number of bad TCP headers detected.
Slow path segments	Number of segments that are sent through the slow path if the TCP segment does not pass fast-path segment validation.
Fast path segments	Number of segments that are sent through the fast path after passing a predefined TCP validation sequence.
Sequence number wrap around errors	Number of packets that wrap around of the sequence number.
Session reuses	Number of sessions that reused an already established TCP session.
SYN retransmissions	Number of SYN packets that are retransmitted.
Bad three way handshake acknowledgements	Number of packets that have incorrect three-way handshake acknowledgements (ACK packet).
Sequence number out of sync flows	Number of packets that have out-of-sync sequence numbers.
Fast path pattern matches in queued up streams	Number of queued packets that have fast path pattern match.

Table 295: show security idp counters tcp-reassembler Output Fields (*continued*)

Field Name	Field Description
New segments with no overlaps with old segment	Number of new segments that do not overlap with old segment.
New segment overlaps with beginning of old segment	Number of new segments that overlap with beginning of old segment.
New segment overlaps completely with old segment	Number of new segments that overlap completely with old segment.
New segment is contained in old segment	Number of new segments contained in old segment.
New segment overlaps with end of old segment	Number of new segments that overlap with the end of old segment.
New segment begins after end of old segment	Number of new segments that overlap after the end of old segment.
Memory consumed by new segment	Memory that is consumed by the new segment.
Segments in memory	Number of segments that are stored in memory for processing.
Per-flow memory overflows	Number of segments dropped after reaching per flow memory limit.
Global memory overflows	Number of segments dropped after reaching reassembler global memory limit.
Overflow drops	Number of packets that are dropped due to memory overflow.
Copied packets (Unsupported)	Number of packets copied in reassembler.
Closed Acks	Number of Ack packets seen without having seen SYN on the same session.

## Sample Output

### show security idp counters tcp-reassembler

```

user@host> show security idp counters tcp-reassembler
IDP counters:
IDP counter type                               Value
Bad TCP checksums                             0
Bad TCP headers                               0
Slow path segments                             4
Fast path segments                             23
Sequence number wrap around errors             0
Session reuses                                0
SYN retransmissions                           0
Bad three way handshake acknowledgements       0
Sequence number out of sync flows             0

```

Fast path pattern matches in queued up streams	0
New segments with no overlaps with old segment	0
New segment overlaps with beginning of old segment	0
New segment overlaps completely with old segment	0
New segment is contained in old segment	0
New segment overlaps with end of old segment	0
New segment begins after end of old segment	0
Memory consumed by new segment	0
Segments in memory	0
Per-flow memory overflows	0
Global memory overflows	0
Overflow drops	0
Copied packets	0
Closed Acks	0

## show security idp logical-system policy-association

<b>Syntax</b>	show security idp logical-system policy-association
<b>Release Information</b>	Command introduced in Junos OS Release 11.3.
<b>Description</b>	Display the IDP policy assigned to a logical system. The IDP policy is assigned to a logical system through the security profile.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>security-profile</i></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>Master Administrator for Logical Systems Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp logical-system policy-association on page 2250</a>
<b>Output Fields</b>	<a href="#">Table 296 on page 2250</a> lists the output fields for the <b>show security idp logical-system policy-association</b> command.

**Table 296: show security idp logical-system policy-association Output Fields**

Field Name	Field Description
Logical system	Name of the logical system to which an IDP policy is assigned.
IDP policy	Name of the IDP policy that is specified in the security profile that is bound to the logical system.

## Sample Output

### show security idp logical-system policy-association

```

user@host> show security idp logical-system policy-association
Logical system      IDP policy
root-logical-system idp-policy1
lsys1               idp-policy2

```

## show security idp memory

<b>Syntax</b>	show security idp memory
<b>Release Information</b>	Command introduced in Junos OS Release 9.2. Percentage outputs added in Junos OS Release 10.1.
<b>Description</b>	Display the status of all IDP data plane memory.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp memory on page 2251</a>
<b>Output Fields</b>	<a href="#">Table 297 on page 2251</a> lists the output fields for the <b>show security idp memory</b> command. Output fields are listed in the approximate order in which they appear.

**Table 297: show security idp memory Output Fields**

Field Name	Field Description
PIC	Name of the PIC.
Total IDP data plane memory	Total memory space that is allocated for the IDP data plane.  <i>NOTE:</i> IDP requires a minimum of 5 MB of memory for session inspection.
Used	Used memory space in the data plane.
Available	Available memory space in the data plane.

## Sample Output

### show security idp memory

```

user@host> show security idp memory
  IDP data plane memory statistics:
    PIC : FPC 0 PIC 0:
Total IDP data plane memory : 196 MB
    Used : 8 MB ( 8192 KB ) ( 4.08% )
    Available : 188 MB ( 192512 KB ) (95.91%)

```

## show security idp policies

---

<b>Syntax</b>	show security idp policies
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Display the list of currently installed policies.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp active-policy on page 99</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li><li>• <i>IDP Class of Service Action Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	user@host> show security idp policies

## Sample Output

```
Subscriber: s0,          Installed policies: 1

  ID      Name      Sessions      Memory      detector
  0       new1       0            10179       9.2.160090324
```

## show security idp policy-commit-status

---

<b>Syntax</b>	show security idp policy-commit-status
<b>Release Information</b>	Command introduced in JUNOS OS Release 10.4.
<b>Description</b>	Display the IDP policy commit status. For example, status of policy compilation or load.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp status on page 100</a></li><li>• <a href="#">show security idp policy-commit-status clear on page 2254</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>

### Sample Output

```
user@host> show security idp policy-commit-status
Reading prereq sensor config...
```

## [show security idp policy-commit-status clear](#)

---

<b>Syntax</b>	show security idp policy-commit-status clear
<b>Release Information</b>	Command introduced in Junos OS Release 10.4.
<b>Description</b>	Clear the IDP policy commit status.
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp policy-commit-status on page 2253</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	This command produces no output.



## show security idp policy-templates

---

<b>Syntax</b>	show security idp policy-templates
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Display the list of available policy templates.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show security idp active-policy on page 99</a></li><li>• <i>IDP Policies Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	user@host> show security idp policy-templates

### Sample Output

```
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Web_Server
```

## show security idp predefined-attacks

---

<b>Syntax</b>	show security idp predefined-attacks filters ( category   severity   direction)
<b>Release Information</b>	Command introduced in Junos OS Release 10.1.
<b>Description</b>	Display information about predefined attacks using optional filters.
<b>Options</b>	filters (Optional) <ul style="list-style-type: none"><li>• <b>category</b>—Show predefined attacks in different categories.</li><li>• <b>severity</b>—Show predefined attacks based on different severities.<ul style="list-style-type: none"><li>• critical</li><li>• info</li><li>• major</li><li>• minor</li><li>• warning</li></ul></li><li>• <b>direction</b> — Show predefined attacks for different directions.<ul style="list-style-type: none"><li>• any</li><li>• client-to-server</li><li>• exclude-any</li><li>• exclude-client-to-server</li><li>• exclude-server-to-client</li><li>• server-to-client</li></ul></li></ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>IDP Policies Feature Guide for Security Devices</i></li><li>• <i>IDP Application Identification Feature Guide for Security Devices</i></li></ul>
<b>Output Fields</b>	user@host> show security idp predefined-attacks filters category APP

## Sample Output

```
APP:AMANDA:AMANDA-ROOT-OF1
APP:AMANDA:AMANDA-ROOT-OF2
APP:ARKEIA:TYPE-77-OF
APP:CA:ALERT-SRV-OF
APP:CA:ARCSRV:TCP-BOF
APP:CA:ARCSRV:UA-OF
APP:CA:IGATEWAY-BOF
```

```
APP:CA:LIC-COMMAND-OF
APP:CA:LIC-GCR-OF
APP:CA:LIC-GETCONFIG-OF
APP:CA:LIC-GETCONFIG-OF2
APP:CA:LIC-PUTOLF-OF
APP:CDE-DTSPCD-OF
APP:DOUBLETAKE
APP:ETHEREAL:DISTCC-OF
APP:HPOVNM:HPOVTRACE-OF
APP:KERBEROS:GSS-ZERO-TOKEN
APP:KERBEROS:KBR-DOS-TCP-2
APP:MDAEMON:FORM2RAW-OF
APP:MERCURY-BOF
APP:MISC:MCAFFEE-SRV-HDR
APP:NTOP-WEB-FS1
APP:PPTP:MICROSOFT-PPTP
APP:REMOTE:TIMBUKTU-AUTH-OF
```

```
user@host> show security idp security-package predefined-attacks filters category FTP
severity critical direction client-to-server
```

```
FTP:COMMAND:WZ-SITE-EXEC
FTP:DIRECTORY:TILDE-ROOT
FTP:EXPLOIT:OPENFTPD-MSG-FS
FTP:OVERFLOW:OPENBSD-FTPD-GLOB
FTP:OVERFLOW:PATH-LINUX-X86-3
FTP:OVERFLOW:WFTPD-MKD-OVERFLOW
FTP:OVERFLOW:WUBSD-SE-RACE
FTP:PROFTP:OVERFLOW1
FTP:PROFTP:PPC-FS2
FTP:SERVU:CHMOD-OVERFLOW
FTP:SERVU:LIST-OVERFLOW
FTP:SERVU:MDTM-OVERFLOW
FTP:WU-FTP:IREPLY-FS
```

## show security idp security-package-version

<b>Syntax</b>	show security idp security-package-version
<b>Release Information</b>	Command introduced in Junos OS Release 9.2.
<b>Description</b>	Display information of the currently installed security package version and detector version.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> <li>• <i>IDP Signature Database Feature Guide for Security Devices</i></li> <li>• <a href="#">security-package on page 2132</a></li> <li>• <a href="#">request security idp security-package download on page 2200</a></li> <li>• <a href="#">request security idp security-package install on page 2202</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp security-package-version on page 2258</a>
<b>Output Fields</b>	<a href="#">Table 298 on page 2258</a> lists the output fields for the <b>show security idp security-package-version</b> command. Output fields are listed in the approximate order in which they appear.

**Table 298: show security idp security-package-version Output Fields**

Field Name	Field Description
Attack database version	Attack database version number that are currently installed on the system.
Detector version	Detector version number that are currently installed on the system.
Policy template version	Policy template version that are currently installed on the system.

## Sample Output

### show security idp security-package-version

```

user@host> show security idp security-package-version
Attack database version:1154(Mon Apr 28 15:08:42 2008)
Detector version :9.1.140080400
Policy template version :7

```

## show security idp ssl-inspection key

<b>Syntax</b>	<code>show security idp ssl-inspection key [&lt;key-name&gt; [server &lt;server-ip&gt;]]</code>
<b>Release Information</b>	Command introduced in Junos OS Release 9.3.
<b>Description</b>	Display SSL keys added to the system along with their associated server IP addresses.
<b>Options</b>	<ul style="list-style-type: none"> <li>• <b>key-name</b> —(Optional) Name of SSL private key.</li> <li>• <b>server server-ip</b> —(Optional) Server IP address associated for specified key.</li> </ul>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp ssl-inspection key on page 2259</a> <a href="#">show security idp ssl-inspection key key2 on page 2259</a>
<b>Output Fields</b>	Table 299 on page 2259 lists the output fields for the <b>show security idp ssl-inspection key</b> command. Output fields are listed in the approximate order in which they appear.

Table 299: show security idp ssl-inspection key Output Fields

Field Name	Field Description
Total SSL keys	Total number of SSL keys.
key	Name of the SSL private key.
server	Server IP address associated with the SSL keys.

## Sample Output

### show security idp ssl-inspection key

```

user@host> show security idp ssl-inspection key
Total SSL keys : 4

SSL Server key and ip address:

Key : key1, server : 1.1.0.1
Key : key1, server : 1.1.0.2
Key : key2, server : 2.2.0.1
key : key3

```

## Sample Output

### show security idp ssl-inspection key key2

```

user@host> show security idp ssl-inspection key key2

```

SSL Server key and ip address:

Key : key2, server : 2.2.0.1

## show security idp ssl-inspection session-id-cache

<b>Syntax</b>	show security idp ssl-inspection session-id-cache
<b>Release Information</b>	Command introduced in Junos OS Release 9.3.
<b>Description</b>	Display all the SSL session IDs in the session ID cache. Each cache entry is 32 bytes long.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear security idp ssl-inspection session-id-cache on page 2198</a></li> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp ssl-inspection session-id-cache on page 2261</a>
<b>Output Fields</b>	<a href="#">Table 300 on page 2261</a> lists the output fields for the <b>show security idp ssl-inspection session-id-cache</b> command. Output fields are listed in the approximate order in which they appear.

**Table 300: show security idp ssl-inspection session-id-cache Output Fields**

Field Name	Field Description
Total SSL session identifiers	Total number of SSL session identifiers stored in the session ID cache.

## Sample Output

### show security idp ssl-inspection session-id-cache

```

user@host> show security idp ssl-inspection session-id-cache
SSL session identifiers :

c98396c768f983b515d93bb7c421fb6b8ce5c2c5c230b8739b7fcf8ce9c0de4e
a211321a3242233243c3dc0d421fb6b8ce5e4e983b515d932c5c230b87392c

Total SSL session identifiers : 2

```

## show security idp status

<b>Syntax</b>	show security idp status
<b>Release Information</b>	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.
<b>Description</b>	Display the status of the current IDP policy.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>IDP Policies Feature Guide for Security Devices</i></li> </ul>
<b>List of Sample Output</b>	<a href="#">show security idp status on page 2263</a>
<b>Output Fields</b>	<a href="#">Table 13 on page 100</a> lists the output fields for the <b>show security idp status</b> command. Output fields are listed in the approximate order in which they appear.

**Table 301: 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"> <li>• min—Minimum delay for a packet to receive and return by a node in microseconds.</li> <li>• max—Maximum delay for a packet to receive and return by a node in microseconds.</li> <li>• ave—Average delay for a packet to receive and return by a node in microseconds.</li> </ul>
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, <b>idp-policy-combined</b> is displayed.
Running Detector Version	Current version of the running detector.
Forwarding process mode	IDP dedicated mode: <b>default</b> , <b>equal</b> , <b>idp</b> , or <b>firewall</b> .



## 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 idp status detail

<b>Syntax</b>	show security idp status detail
<b>Release Information</b>	Command introduced in Junos OS Release 10.1. Output changed to support IDP dedicated mode in Junos OS Release 11.2.
<b>Description</b>	Display statistics for each Services Processing Unit (SPU), including multiple detector information for each SPU.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>IDP Policies Feature Guide for Security Devices</i></li> </ul>

### Sample Output

#### show security idp status detail

```

user@host> show security idp status detail
  PIC : FPC 1 PIC 1:
State of IDP: Default, Up since: 2011-03-29 17:25:07 UTC (00:02:48 ago)

Packets/second: 0                      Peak: 0 @ 2011-03-29 17:25:07 UTC
KBits/second  : 0                      Peak: 0 @ 2011-03-29 17:25:07 UTC
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 @ 2011-03-29 17:25:07 UTC]
  TCP:  [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]
  UDP:  [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]
  Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:07 UTC]

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

Number of SSL Sessions : 0

  PIC : FPC 1 PIC 0:

State of IDP: Default, Up since: 2011-03-29 17:25:08 UTC (00:02:47 ago)

Packets/second: 0                      Peak: 0 @ 2011-03-29 17:25:08 UTC
KBits/second  : 0                      Peak: 0 @ 2011-03-29 17:25:08 UTC
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 @ 2011-03-29 17:25:08 UTC]
  TCP:  [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]
  UDP:  [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]

```

Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:08 UTC]

Session Statistics:

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

Number of SSL Sessions : 0

PIC : FPC 0 PIC 1:

State of IDP: Default, Up since: 2011-03-29 17:25:04 UTC (00:02:51 ago)

Packets/second: 0 Peak: 0 @ 2011-03-29 17:25:04 UTC

KBits/second : 0 Peak: 0 @ 2011-03-29 17:25:04 UTC

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 @ 2011-03-29 17:25:04 UTC]

TCP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]

UDP: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]

Other: [Current: 0] [Max: 0 @ 2011-03-29 17:25:04 UTC]

Session Statistics:

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

Number of SSL Sessions : 0

PIC : FPC 1 PIC 1:

Policy Name : none

PIC : FPC 1 PIC 0:

Policy Name : none

PIC : FPC 0 PIC 1:

Policy Name : none

Forwarding process mode : maximizing sessions firewall



## PART 7

# Standards Reference

- [Overview on page 2269](#)
- [Supported Standards on page 2271](#)



## CHAPTER 22

# Overview

- [Accessing Standards Documents on page 2269](#)

### Accessing Standards Documents

---

- [Accessing Standards Documents on the Internet on page 2269](#)

#### 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 23

# Supported Standards

- [Chassis and System Standards on page 2271](#)
- [Interface Standards on page 2284](#)
- [Layer 2 Standards on page 2289](#)
- [MPLS Applications Standards on page 2291](#)
- [Packet Processing Standards on page 2296](#)
- [Routing Protocol Standards on page 2298](#)
- [Services PIC and DPC Standards on page 2309](#)
- [VPLS and VPN Standards on page 2313](#)

## Chassis and System Standards

---

- [Supported BOOTP and DHCP Standards on page 2271](#)
- [Supported Mobile IP Standards on page 2272](#)
- [Supported Network Management Standards on page 2273](#)
- [Supported RADIUS and TACACS+ Standards for User Authentication on page 2282](#)
- [Supported System Access Standards on page 2283](#)
- [Supported Time Synchronization Standard on page 2283](#)

## 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 2269](#)

## 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 2269](#)

## 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

Gigabit Ethernet interfaces on J Series Services Routers do not support the 802.3ad MIB.

- 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:

- **sysApplElmtRunTable**
- **sysApplInstallElmtTable**
- **sysApplInstallPkgTable**
- **sysApplMapTable**
- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2466, *Management Information Base for IP Version 6: ICMPv6 Group*

- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types*

The following MIB objects are not supported:

- **dsx1FarEndConfigTable**
- **dsx1FarEndCurrentTable**
- **dsx1FarEndIntervalTable**
- **dsx1FarEndTotalTable**
- **dsx1FracTable**

- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type*

The following MIB objects are not supported:

- **dsx3FarEndConfigTable**
- **dsx3FarEndCurrentTable**
- **dsx3FarEndIntervalTable**
- **dsx3FarEndTotalTable**
- **dsx3FracTable**

- RFC 2515, *Definitions of Managed Objects for ATM Management*

The following MIB objects are not supported:

- **aal5VccTable**
- **atmVcCrossConnectTable**
- **atmVpCrossConnectTable**

- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type* (obsoleted by RFC 3592)

- RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

Only read-only access is supported.

- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (obsoleted by RFC 3412)

Only read-only access is supported.

- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2662, *Definitions of Managed Objects for the ADSL Lines*

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
- **mplsTunnelCRLDPResTable** 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 2269](#)

## 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 2283](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2282](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2269](#)

## Interface Standards

---

- [Supported ATM Interface Standards on page 2284](#)
- [Supported Ethernet Interface Standards on page 2284](#)
- [Supported Frame Relay Interface Standards on page 2285](#)
- [Supported GRE and IP-IP Interface Standards on page 2286](#)
- [Supported PPP Interface Standards on page 2286](#)
- [Supported SDH and SONET Interface Standards on page 2287](#)
- [Supported Serial Interface Standards on page 2288](#)
- [Supported T3 Interface Standard on page 2288](#)

### 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 2269](#)

### 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## Layer 2 Standards

- [Supported Layer 2 Networking Standards on page 2289](#)
- [Supported L2TP Standards on page 2289](#)
- [Supported Layer 2 Circuit Standards on page 2290](#)
- [Supported Layer 2 VPN Standard on page 2290](#)

### 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 2289](#)
- [Supported Layer 2 Circuit Standards on page 2290](#)
- [Supported Layer 2 VPN Standard on page 2290](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

### 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 2269](#)

## 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 2313](#)
- [Supported Layer 2 VPN Standard on page 2290](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported Multicast VPN Standards on page 2315](#)
- [Supported VPLS Standards on page 2315](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2313](#)
- [Supported Layer 2 Circuit Standards on page 2290](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported Multicast VPN Standards on page 2315](#)
- [Supported VPLS Standards on page 2315](#)

- [Accessing Standards Documents on the Internet on page 2269](#)

## MPLS Applications Standards

- [Supported GMPLS Standards on page 2291](#)
- [Supported LDP Standards on page 2292](#)
- [Supported MPLS Standards on page 2293](#)
- [Supported RSVP Standards on page 2295](#)

## 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 [sic] 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 [sic] Label Switching (GMPLS) Signaling Resource ReserVation [sic] Protocol-Traffic Engineering (RSVP-TE) Extensions*

Only Section 9, "Fault Handling," is supported.

- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol [sic] Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, *Routing Extensions in Support of Generalized Multi-Protocol [sic] 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 [sic] 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 [sic] 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 2292](#)
- [Supported MPLS Standards on page 2293](#)
- [Supported RSVP Standards on page 2295](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## Supported LDP Standards

The Junos OS substantially supports the following RFCs, which define standards for LDP.

- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*

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, the Junos OS supports one of the possible modes but not the other:

- 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 2291](#)
  - [Supported MPLS Standards on page 2293](#)
  - [Supported RSVP Standards on page 2295](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## Supported MPLS Standards

The 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 [sic] Label Switching (MPLS) Support of Differentiated Services*  
Only E-LSPs are supported.
- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol [sic] 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 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 [sic] Label Switched (MPLS) Data Plane Failures*  
The traceroute functionality is supported only on transit routers.
- RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*
- Internet draft draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*
- Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)
- 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 3063, *MPLS Loop Prevention Mechanism*

- RFC 3208, *PGM Reliable Transport Protocol Specification*

Only the network element is supported.

- RFC 3469, *Framework for Multi-Protocol [sic] 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*

The 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 which 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 2291](#)
- [Supported LDP Standards on page 2292](#)
- [Supported RSVP Standards on page 2295](#)
- [Accessing Standards Documents on the Internet on page 2269](#)



## Supported RSVP Standards

The Junos OS substantially supports the following RFCs and Internet drafts, which define standards for RSVP.

- RFC 2205, *Resource ReSerVation [sic] 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 [sic] Label Switching (GMPLS) Signaling Resource ReserVation [sic] Protocol-Traffic Engineering (RSVP-TE) Extensions*

Only Section 9, “Fault Handling,” is supported.

- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation [sic] Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

Node protection in facility backup is not supported.

- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol [sic] 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.

- Internet draft draft-ietf-mppls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)

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 [sic] 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 2291](#)
- [Supported LDP Standards on page 2292](#)
- [Supported MPLS Standards on page 2293](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

---

## Packet Processing Standards

- [Supported CoS Standards on page 2296](#)
- [Supported Packet Filtering Standards on page 2297](#)
- [Supported Policing Standard on page 2297](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

---

## Routing Protocol Standards

- [Supported BGP Standards on page 2298](#)
- [Supported ES-IS Standards on page 2300](#)
- [Supported ICMP and Neighbor Discovery Standards on page 2300](#)
- [Supported IP Multicast Protocol Standards on page 2301](#)
- [Supported IPv4, TCP, and UDP Standards on page 2302](#)
- [Supported IPv6 Standards on page 2303](#)
- [Supported IS-IS Standards on page 2306](#)
- [Supported OSPF and OSPFv3 Standards on page 2307](#)
- [Supported RIP and RIPng Standards on page 2309](#)

### Supported BGP Standards

The 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 2303.

Junos 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 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 4659, *BGP/MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4486, *Subcodes for BGP Cease Notification Message*
- RFC 4724, *Graceful Restart Mechanism for BGP*
- RFC 4760, *Multiprotocol Extensions for BGP-4*
- RFC 4781, *Graceful Restart Mechanism for BGP with MPLS*
- RFC 4893, *BGP Support for Four-octet AS Number Space*
- 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 5396, *Textual Representation of Autonomous System (AS) Numbers*
- RFC 5668, *4-Octet AS Specific BGP Extended Community*
- 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-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*
- Internet draft draft-ietf-idr-add-paths-04.txt, *Advertisement of Multiple Paths in BGP* (expires February 2011)
- Internet draft draft-ietf-idr-aigp-06, *The Accumulated IGP Metric Attribute for BGP* (expires December 2011)

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 2303](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## 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 [sic] 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 2269](#)

## 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 2302](#)
  - [Supported IPv6 Standards on page 2303](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## 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*
- Internet draft draft-ietf-l3vpn-2547bis-mcast-10.txt, *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 2269](#)

## Supported IPv4, TCP, and UDP Standards

The Junos OS substantially supports the following RFCs, which define standards for IP version 4 (IPv4), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

- RFC 768, *User Datagram Protocol*
- RFC 791, *INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 793, *TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 826, *Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*
- RFC 854, *TELNET PROTOCOL SPECIFICATION*
- RFC 862, *Echo Protocol*
- RFC 863, *Discard Protocol*
- RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*
- RFC 896, *Congestion Control in IP/TCP Internetworks*



- RFC 903, *A Reverse Address Resolution Protocol*
- RFC 919, *BROADCASTING INTERNET DATAGRAMS*
- RFC 922, *BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*
- RFC 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 2303](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## Supported IPv6 Standards

The Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP 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-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 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 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*

IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2472, *IP Version 6 over PPP*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

- RFC 2491, *IPv6 Over Non-Broadcast Multiple Access (NBMA) networks*
  - RFC 2492, *IPv6 over ATM Networks*
  - RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
  - RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
  - RFC 2578, *Structure of Management Information Version 2 (SMIPv2)*
  - RFC 2675, *IPv6 Jumbograms*
  - RFC 2711, *IPv6 Router Alert Option*
  - RFC 2740, *OSPF for IPv6*
  - RFC 2878, *PPP Bridging Control Protocol (BCP)*
  - RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*
  - RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- Address assignment is supported with IP version 4 (IPv4) but not IP version 6 (IPv6).
- RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*
  - RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
  - RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*
  - RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
  - draft-ietf-vrrp-unified-spec-02.txt *Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6*
  - RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
  - RFC 4291, *IP Version 6 Addressing Architecture*
  - RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
  - RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
  - RFC 4861, *Neighbor Discovery for IP Version 6 (IPv6)*
  - RFC 4862, *IPv6 Stateless Address Autoconfiguration*
  - RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*
  - RFC 5308, *Routing IPv6 with IS-IS*
  - Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
  - Internet 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*
  - 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.

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-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP*

Only MP-BGP over IP version 4 (IPv4) approach is supported.

**Related  
Documentation**

- [Supported IPv4, TCP, and UDP Standards on page 2302](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2300](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## Supported OSPF and OSPFv3 Standards

The 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*
- 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 [sic] 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 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- 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 and Internet drafts 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 2303](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2302](#)
- [Supported IPv6 Standards on page 2303](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

---

## Services PIC and DPC Standards

- [Supported DTCP Standard on page 2309](#)
- [Supported Flow Monitoring and Discard Accounting Standards on page 2310](#)
- [Supported IPsec and IKE Standards on page 2310](#)
- [Supported L2TP Standards on page 2311](#)
- [Supported Link Services Standards on page 2311](#)
- [Supported NAT and SIP Standards on page 2312](#)
- [Supported RPM Standard on page 2312](#)
- [Supported Voice Services Standards on page 2313](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## 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 2269](#)

## VPLS and VPN Standards

- [Supported Carrier-of-Carriers and Interprovider VPN Standards on page 2313](#)
- [Supported Layer 2 VPN Standard on page 2313](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported Multicast VPN Standards on page 2315](#)
- [Supported VPLS Standards on page 2315](#)

## 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 2290](#)
- [Supported Layer 2 VPN Standard on page 2290](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported Multicast VPN Standards on page 2315](#)
- [Supported VPLS Standards on page 2315](#)
- [Supported BGP Standards on page 2298](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2313](#)
  - [Supported Layer 2 Circuit Standards on page 2290](#)
  - [Supported Layer 3 VPN Standards on page 2314](#)
  - [Supported Multicast VPN Standards on page 2315](#)
  - [Supported VPLS Standards on page 2315](#)
  - [Accessing Standards Documents on the Internet on page 2269](#)

## 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 [sic] 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 [sic] 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 2313](#)
  - [Supported Layer 2 Circuit Standards on page 2290](#)
  - [Supported Layer 2 VPN Standard on page 2290](#)
  - [Supported Multicast VPN Standards on page 2315](#)
  - [Supported VPLS Standards on page 2315](#)
  - [Supported MPLS Standards on page 2293](#)
  - [Supported BGP Standards on page 2298](#)
  - [OSPF Features in the Junos OS](#)

- [Accessing Standards Documents on the Internet on page 2269](#)

## Supported Multicast VPN Standards

The Junos OS substantially supports the following Internet drafts, which define standards for multicast virtual private networks (VPNs).

- Internet draft draft-ietf-l3vpn-2547bis-mcast-10.txt, *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 2313](#)
- [Supported Layer 2 Circuit Standards on page 2290](#)
- [Supported Layer 2 VPN Standard on page 2290](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported VPLS Standards on page 2315](#)
- [Supported MPLS Standards on page 2293](#)
- [Supported BGP Standards on page 2298](#)
- [Accessing Standards Documents on the Internet on page 2269](#)

## 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 2313](#)
- [Supported Layer 2 Circuit Standards on page 2290](#)
- [Supported Layer 2 VPN Standard on page 2290](#)
- [Supported Layer 3 VPN Standards on page 2314](#)
- [Supported Multicast VPN Standards on page 2315](#)
- [Accessing Standards Documents on the Internet on page 2269](#)



## PART 8

# Index

- [Index on page 2319](#)





# Index

## Symbols

!	
in interface names.....	349
regular expression operator	
system logging.....	1665
" ", configuration group wildcards.....	435
#, comments in configuration statements.....	lx, 390
\$	
regular expression operator	
system logging.....	1665
()	
regular expression operator	
system logging.....	1665
( ), in syntax descriptions.....	lx
*	
in interface names.....	349
regular expression operator.....	516
system logging.....	1665
wildcard character.....	435
* (red asterisk).....	582
+	
in statement lists.....	381
regular expression operator.....	516
system logging.....	1665
.	
regular expression operator	
system logging.....	1665
. (period)	
regular expression operator.....	516
/* */, comment delimiters.....	390
/cf/var/crash directory See crash files	
/cf/var/log directory See system logs	
/cf/var/tmp directory See temporary files	
/var/log directory See system log messages	
/var/log/mib2d file.....	1968
/var/log/snmpd file.....	1968
< >, in syntax descriptions.....	lx
?	
regular expression operator.....	435
system logging.....	1665
wildcard.....	435

? icon .....	582
[ ]	
regular expression operator	
system logging.....	1665
[ ], in configuration statements.....	lx
\	
in interface names.....	349
wildcard characters.....	435
^	
regular expression operator	
system logging.....	1665
{ }, in configuration statements.....	lx
specifying statements.....	344
regular expression operator	
system logging.....	1665
(pipe).....	533
command output.....	533
in syntax descriptions.....	lx, 533
(pipe) command.....	1231
(pipe), in syntax descriptions.....	lx, 533

## A

AAA Objects MIB.....	1733, 1745, 1751
Access Authentication Objects	
MIB.....	1733, 1740, 1745, 1751
access privilege levels	
configuration example.....	1070
configuration mode	
hierarchies.....	1070, 1075
operational mode commands.....	1074
configuring.....	1067
configuration mode	
hierarchies.....	1066, 1069
operational mode commands.....	1067
entering configuration mode.....	358
login classes.....	1059
access privileges	
denying and allowing commands.....	675
permission bits for.....	673
predefined.....	673
specifying.....	902
access statement	
usage guidelines.....	1853
access, configuration summary.....	595
access-list statement.....	1887
accounting options	
configuration.....	1254
configuration summary.....	595

overview.....	1235	alarm class See alarm severity	
sample task.....	608	ALARM LED, color.....	1237
accounting profiles		Alarm MIB.....	1733, 1740, 1745, 1751
filter.....	1263	alarm severity	
interface.....	1260	configuring for an interface.....	1276
MIB.....	1272	major (red) .....	1237
Routing Engine.....	1274	See also major alarms	
accounting-options statement.....	1315	minor (yellow).....	1237
accounts See template accounts; user accounts		See also minor alarms	
ack-number statement.....	2017	alarm statement	
action statement.....	2019	RMON.....	1890
(Security Application-Level DDoS).....	2018	usage guidelines.....	1871
action-profile statement.....	1316, 2021	alarms.....	1592
activate command.....	535	active, displaying at login.....	1276
usage guidelines.....	336	chassis.....	616
activate statements and identifiers.....	388	conditions, on an interface.....	1238
active configuration.....	311	configurable.....	1238
active-policy statement.....	2020	configuration requirements for interface	
adaptive services interfaces		alarms.....	1276
alarm conditions and configuration		interface.....	616
options.....	1238	licenses.....	1241
Add new entry link.....	606	major.....	616, 1237 See major alarms
address statement		minor.....	616, 1237 See minor alarms
SNMPv3.....	1888	overview.....	1237
usage guidelines.....	1847	red.....	616, 1237 See major alarms
Address-Assignment Pool		rescue configuration.....	1241
pool name.....	724, 731	severity.....	616, 1477, 1478 See alarm severity
Address-Assignment Pools.....	724, 731	system.....	616
address-assignment pools		type.....	616
client attributes.....	749	types.....	1237
configuring overview.....	745	verifying.....	1278
DHCP attributes.....	749	viewing, sample.....	616
dhcpv6 attributes.....	749	yellow.....	616, 1237 See minor alarms
linking.....	748	alarms sample task.....	616
named range.....	748	alert logging severity.....	619
router advertisement.....	750	alert statement.....	2022
address-assignment statement.....	769	alias, CoS value.....	1369
address-mask statement.....	1888	allow-commands statement	
usage guidelines.....	1847	usage guidelines.....	1062
address-pool statement.....	772	allow-configuration statement.....	773
addresses		allow-configuration-regexps statement.....	774
machine name.....	372	usage guidelines.....	1062
administrative roles		allow-duplicates statement.....	1668
example.....	914	allow-icmp-without-flow statement.....	2022
advanced BGP feature, license.....	624	allowing commands to login classes.....	1062
AES encryption		annotate command.....	336, 536
setting.....	932	usage guidelines.....	390
agent, SNMP.....	1718	anomaly statement.....	2023
agent-address statement.....	1889		

- 
- ANSI standards supported *See* Index of Supported Software Standards
- any (system logging facility).....1642
- any (system logging severity level).....1643
- application (Security IDP).....2024
- application statement
- (Security Application-Level DDoS).....2024
  - (Security Custom Attack).....2023
- application-ddos statement.....2025
- application-identification statement.....2026
- application-level DDoS rule statement.....2124
- applications, configuration summary.....595
- apply-groups statement.....461
- usage guidelines.....429
- apply-groups-except statement.....461
- archive statement
- all system log files.....1669
- archive-sites statement
- accounting.....1317
  - usage guidelines.....1260
- archiving files.....960
- arithmetic and relational operators
- for monitor traffic command.....1521
- arithmetic operators, for multicast traffic.....1503
- AS path, displaying.....1415
- AT commands, for modem initialization
- description.....678
- ATM CoS MIB.....1734, 1745, 1751
- ATM interfaces
- supported software standards.....2284
- ATM MIB.....1734
- attack-type (Security IDP).....2030
- attack-type statement
- (Security Anomaly).....2027
  - (Security Chain).....2028
  - (Security Signature).....2034
- attacks
- brute force, preventing.....923
  - dictionary, preventing.....923
- attacks statement
- (Security Exempt Rulebase).....2038
  - (Security IPS Rulebase).....2039
- authentication
- local password, by default.....900
  - login classes.....673, 902
  - methods.....671, 672
  - order of user authentication (configuration editor).....900
  - RADIUS authentication (configuration editor).....895
  - specifying a method.....900
  - specifying access privileges.....902
  - TACACS+ authentication (configuration editor).....897
  - user accounts.....672, 902
- authentication-key statement.....775
- authentication-md5 statement.....1891
- usage guidelines.....1830
- authentication-none statement.....1892
- usage guidelines.....1831
- authentication-order statement.....776
- authentication-password statement.....1893
- usage guidelines.....1830
- authentication-sha statement.....1894
- usage guidelines.....1830
- authorization *See* permissions
- authorization (system logging facility).....1642
- authorization statement.....1895
- usage guidelines.....1862
- auto-prefix delegation.....739
- autoinstallation.....246
- automatic configuration process.....153
  - CLI configuration editor.....205
  - default configuration file.....153
  - establishing.....151
  - host-specific configuration file.....153
  - interfaces.....152
  - IP address procurement process.....153
  - J-Web configuration editor.....205
  - overview.....151, 156
  - protocols for procuring an IP address.....152
  - requirements.....205
  - status.....207
  - TFTP server.....153
  - verifying.....207
- autoinstallation, compatibility with the DHCP server.....687
- automatic configuration *See* autoinstallation
- automatic statement.....2040
- Avaya VoIP
- troubleshooting.....1627
  - version incompatibility, correcting.....1627
- B**
- backing up current installation
- J Series Services Routers.....171

backup		branch SRX	
boot device.....	625	factory default	
current configuration.....	625	configuration.....	34
rescue configuration.....	625	licenses.....	48
system software.....	625	reset.....	38
basic connectivity		brief statement	
Quick Configuration.....	588	system logging.....	1688
requirements.....	588	usage guidelines.....	1659
secure Web access.....	663	broadcast messages, synchronizing NTP.....	779
selecting.....	627	broadcast statement.....	778
batch commit		broadcast-client statement.....	779
usage guidelines.....	352, 414	browser	
BFD MIB.....	1734, 1741, 1746, 1751	downloading software.....	172
BGP		browser interface See J-Web interface	
supported software standards.....	2298	brute force attacks, preventing.....	923
BGP (Border Gateway Protocol)		built-in Ethernet ports See Ethernet ports;	
monitoring.....	1419	management interfaces	
peers, probes to See BGP RPM probes		buttons	
RPM probes to BGP neighbors See BGP RPM		Cancel (J-Web configuration	
probes		editor).....	584, 607
statistics.....	1419	Commit (J-Web configuration	
BGP groups, displaying.....	1419	editor).....	584, 607
BGP neighbors		Discard (J-Web configuration editor).....	607
directing RPM probes to.....	1303	OK (J-Web configuration editor).....	584, 607
displaying.....	1419	Refresh (J-Web configuration editor).....	607
monitoring with RPM probes.....	1301	bypass LSPs, testing.....	1541
BGP peers See BGP neighbors			
BGP routing information.....	1419	<b>C</b>	
BGP RPM probes		cables	
directing to select BGP neighbors		console port, connecting.....	1612
(configuration editor).....	1303	Ethernet rollover, connecting.....	1612
overview.....	1252	cache-size statement	
setting up on local and remote device		(Security).....	2040
(configuration editor).....	1301	Cancel button.....	607
BGP sessions, status.....	1419	J-Web configuration editor.....	584
BGP4 V2 MIB.....	1734, 1740, 1745, 1751	candidate configuration.....	311
binary operators, for multicast traffic.....	1503	capture-file statement.....	1318
binary security log file.....	1645	capturing packets See packet capture	
boot-server statement		categories statement.....	1895
NTP.....	777	usage guidelines.....	1841
BOOTP		category change software installation.....	136
supported software standards.....	2271	category statement	
BOOTP, for autoinstallation.....	205	(Security Dynamic Attack Group).....	2041
braces, in configuration statements.....	lx	certificates See SSL certificates	
brackets		chain statement.....	2042
angle, in syntax descriptions.....	lx	change-log (system logging facility).....	1642
square, in configuration statements.....	lx		

- chassis
  - configuration summary.....595
  - monitoring.....637, 1448
  - power management.....1448
- chassis cluster.....13
- Chassis Cluster MIB.....1735, 1746, 1752
- Chassis Definitions for Router Model MIB.....1734
- Chassis Forwarding MIB.....1734
- Chassis MIB.....1734, 1741, 1746, 1752
- chassis viewer.....628
- chassis-control
  - restart options.....265
- checksum
  - calculating for a file.....962, 963, 964
- ciphers.....870
- Class 1 MIB objects.....1769
- Class 2 MIB objects.....1773
- Class 3 MIB objects.....1774
- Class 4 MIB objects.....1775
- class of service (CoS)
  - configuration summary.....596
  - monitoring.....629
- class statement
  - usage guidelines.....1063
- Class-of-Service MIB.....1735
- class-usage-profile statement.....1319
  - usage guidelines.....1270
- classifiers, CoS.....1368, 1375
- cleaning up files.....649, 934, 935
- clear dhcp client binding command.....949
- clear dhcp client statistics command.....951
- clear dhcp relay binding command.....953
- clear dhcp relay statistics command.....954
- clear dhcp server binding command.....955
- clear dhcp server statistics command.....956
- clear dhcpv6 server binding command.....957
- clear dhcpv6 server statistics command.....958
- clear log command.....1699
- clear security datapath-debug counters
  - command.....2185
- clear security idp .....2186
- clear security idp application-ddos cache.....2187
- clear security idp attack table command.....2188
- clear security idp counters application-identification
  - command.....2189
- clear security idp counters dfa command.....2190
- clear security idp counters flow command.....2191
- clear security idp counters http-decoder
  - command.....2192
- clear security idp counters ips command.....2193
- clear security idp counters log command.....2194
- clear security idp counters packet command.....2195
- clear security idp counters policy-manager
  - command.....2196
- clear security idp counters tcp-reassembler
  - command.....2197
- clear security idp ssl-inspection session-id-cache
  - command.....2198
- clear security log file command.....1702
- clear security logcommand.....1700
- clear system login lockout command.....959
- clear system services dhcp conflicts
  - command.....688
- cli.....6
- CLI See Junos OS CLI
  - command completion.....518
  - command history.....455
    - displaying.....532
  - comparing configuration versions.....571
  - configuration mode
    - description.....335
    - navigation commands, table.....313
  - current working directory
    - displaying.....531
    - setting.....519
  - date
    - setting.....527
  - editing command line.....347
  - idle timeout, setting.....520
  - keyboard sequences.....347
  - permissions, displaying.....530, 1227
  - prompt strings.....510
  - prompt, setting.....521
  - restart, after software upgrade.....522
  - screen length, setting.....523
  - screen width, setting.....524
  - settings, displaying.....528
  - terminal type, setting.....525
  - timestamp.....510
  - timestamp, setting.....526
  - type checking.....346
  - users, monitoring.....497
  - word history.....455
  - working directory.....510
- CLI configuration editor
  - autoinstallation.....205
  - controlling user access.....902
  - interface alarms.....1276

RADIUS authentication.....	895	commands	
RPM.....	1294	allowing or denying to login classes.....	1062
secure access configuration.....	892	completion.....	318, 511
system log messages, sending to a file.....	1652	configure.....	511
TACACS+ authentication.....	897	filenames, specifying.....	500
CLI terminal.....	601	help about.....	315
overview.....	601	history.....	455
starting.....	600	options.....	322
clickable configuration See J-Web configuration		URLs, specifying.....	500
editor		comments	
client attributes		adding to configuration file.....	390
address-assignment pools.....	749	comments, in configuration statements.....	lx
client list		commit and-quit command	
adding to SNMP community.....	1863	usage guidelines.....	408
client-ia-type statement.....	779	commit at command	
client-identifier (dhcp-client) statement.....	780	usage guidelines.....	410
client-identifier statement.....	780	Commit button.....	584, 607
client-list statement.....	1896	commit command.....	537
usage guidelines.....	1863	usage guidelines.....	336, 406
client-list-name statement.....	781, 1896	commit comment command	
usage guidelines.....	1863	usage guidelines.....	412
client-type statement.....	781	commit confirmed command	
clients statement.....	1897	usage guidelines.....	409
usage guidelines.....	1862	commit operations, pending	
code point aliases, CoS.....	1369	displaying.....	567
code statement.....	2043	commit scripts.....	314
command history		commit statement.....	483
operational mode.....	455	commit synchronize command.....	537
command output		commit   display detail command	
configuration details.....	364	usage guidelines.....	411
configuration, comparing files.....	329	commit-delay statement.....	1897
end of, displaying from.....	332	usage guidelines.....	1817
filtering		commit-interval statement.....	462
comparing configuration versions.....	571	committed configuration	
number of lines, counting.....	330	comparing two configurations.....	646
pagination, preventing.....	333	methods.....	644
regular expressions		overview.....	593, 603
first match, displaying from.....	331	rescue configuration .....	648
matching output, displaying.....	332	storage location.....	594, 604
nonmatching output, ignoring.....	331	summaries.....	643
retaining.....	332	committing a configuration.....	593, 603
RPC, displaying.....	331	committing configuration	
saving to a file.....	334	and exiting configuration mode.....	408
sending to users.....	333	basic.....	406
XML format, displaying.....	330	confirmation required.....	409
command shell.....	309	logging message about.....	412
command-line interface See Junos OS CLI		monitoring.....	411
downloading software.....	173	scheduling for later.....	410
		synchronizing on Routing Engines.....	426

- community statement
  - RMON.....1899
    - usage guidelines.....1874
  - SNMP.....1898
    - usage guidelines.....1862
- community string, SNMP.....1862
- community-name statement.....1900
  - usage guidelines.....1865
- compare command.....533
  - usage guidelines.....571
- compare filter.....329
- comparing files.....965
- completing partial command entry.....518
- compressing files.....960
- configuration
  - activating.....569
  - adding comments.....390
  - autoinstallation of.....151
  - candidate.....311
  - committing.....406, 607
    - and exiting configuration mode.....408
    - confirmation required.....409
    - logging message about.....412
    - monitoring process.....411
    - scheduling for later.....410
    - synchronizing on Routing Engines.....426
  - committing as a text file, with caution .....599
  - comparing with previous.....571
  - deleting
    - statements.....382
  - discarding changes .....607
  - displaying
    - current configuration.....559, 1548
    - details.....364
  - downgrading software (CLI).....199
  - downgrading software (J-Web).....199
  - downloading .....646
  - edit command, using.....341
  - editing .....595, 604
  - editing as a text file, with caution .....599
  - global replacement.....349
  - groups configuration groups *See* configuration groups
  - installation on multiple devices.....151
  - loading previous .....645
  - locking.....367
  - merging current and new.....422
  - modifying.....341
  - previous, displaying.....570
  - protecting.....399
  - replacing.....422
  - rollback .....645
  - saving to file.....573
  - storage of previous.....354
  - unprotecting.....399
  - upgrading (CLI).....177
  - uploading .....647
  - users-editors, viewing.....644
  - validation.....23, 32
  - verification.....24, 33
  - viewing as a text file .....597
  - zones and policies.....39
- configuration database, summary.....645
- configuration files
  - automatic installation.....154
  - decrypting.....695
  - encrypting.....695
  - filename, specifying.....500
  - saving to files.....573
  - URL, specifying.....500
- configuration groups
  - applying.....429
  - creating.....428
  - inheritance model.....354
  - inherited values.....433
  - interface parameters.....442, 444
  - nested groups.....430
  - overview.....353
  - peer entities.....445
  - re0, re1 groups.....428
  - regional configurations.....447
  - sets of statements.....440
  - wildcards.....435, 448
- configuration hierarchy, J-Web display.....583
- configuration history
  - comparing files.....646
  - database summary.....645
  - downloading files.....646
  - summary.....643
  - users-editors, viewing.....644
- Configuration History page.....643
- Configuration Management
  - MIB.....1735, 1741, 1746, 1752
- configuration mode, CLI.....381, 406
  - command completion.....318
  - commands
    - activate.....336
    - annotate.....336



commit.....	336
copy.....	336
deactivate.....	336
delete.....	336
edit.....	336
exit.....	336
extension.....	336
help.....	336
insert.....	336
load.....	336
paste.....	337
quit.....	337
rollback.....	337, 575
run.....	337
save.....	337
set.....	337
show.....	337
status.....	337
top.....	337
up.....	337
update.....	337
configuration hierarchy, description.....	339
description.....	335
entering.....	358
example .....	374
exiting.....	359
global replacement.....	349
identifier, description.....	338
locking.....	367
statement	
container.....	339
description.....	338
leaf.....	339
switching to operational mode.....	370
top level statements, interpreting.....	338
users editing configuration	
displaying.....	364
multiple simultaneous users.....	341, 351
configuration mode, entering.....	540
configuration sample tasks	
accounting options.....	608
configuration statements	
adding comments about.....	390
deleting.....	382
help about.....	316
inheriting from groups.....	440
overviews.....	380
structure and components.....	344
configuration text	
editing and committing, with caution.....	599
viewing.....	597
configuration-servers.....	247
configure command.....	540
names and addresses.....	372
usage guidelines.....	320, 358, 513
configure exclusive command	
usage guidelines.....	367
configure link.....	606
configuring	
log suppression.....	1996
configuring address-assignment pool	
dhcpv6.....	745
conflict-log (system logging facility).....	1642
connecting device	
console port.....	16, 25
first time.....	16
connections	
testing	
MPLS Layer 2 circuit connections.....	1531
MPLS Layer 2 VPN connections.....	1528
MPLS Layer 3 VPN connections.....	1534
MPLS LDP connections.....	1536
MPLS LSP-endpoint connections.....	1539
MPLS RSVP connections.....	1541
connectivity	
losing, after initial configuration.....	651
lost DHCP lease after initial	
configuration.....	589
console port.....	6
adapter.....	1612
disabling.....	681
securing.....	681
console statement	
system logging.....	1671
usage guidelines.....	1660
contact statement.....	1901
usage guidelines.....	1815
container hierarchy See hierarchy	
Content Filtering	
verifying.....	1374
content-decompression-max-memory-kb	
statement.....	2044
content-decompression-max-ratio	
statement.....	2045
context statement	
(Security Custom Attack).....	2045
control plane logs.....	1644



controlling user access.....902

conventions

- text and syntax.....lix

copy command.....542

- usage guidelines.....320, 336, 512, 513

copying

- files.....968

CoS See class of service

- MIB.....1735
- supported software standards.....2296

CoS (class of service)

- classifiers.....1368, 1375
- CoS value aliases.....1369
- forwarding classes.....1371
- interfaces.....1367
- loss priority.....1373
- packet loss priority.....1373
- RED drop profiles.....1370
- rewrite rules.....1372
- RPM probe classification.....1298
- See also TCP RPM probes; UDP RPM probes
- scheduler maps.....1373

CoS components for link services

- applying on constituent links.....1617

count command.....533

count filter.....330

count statement

- (Security Custom Attack).....2046

counters statement.....1320

crash files

- cleaning up (CLI).....935
- cleaning up (J-Web).....934
- downloading (J-Web).....937

crash files, cleaning up.....649

critical logging severity.....619

curly braces, in configuration statements.....lx

current working directory

- displaying.....531
- setting.....519

cursor, moving.....347

custom-attack statement.....2047

custom-attack-group statement.....2052

custom-attack-groups (Security IDP).....2052

custom-attacks statement.....2053

customer support.....lix

- contacting JTAC.....lix
- system information, displaying.....995

## D

daemon (system logging facility).....1642

data plane logs.....1644

data types, CLI.....346

data-length statement.....2053

Database Information page.....643

datapath-debug

- security.....1321, 2054

datapath-debug statement.....1321, 2054

date

- setting from CLI.....527

days-to-keep-error-logs statement.....465

deactivate command.....466

- usage guidelines.....336

deactivate statements and identifiers

- usage guidelines.....388

debug logging severity.....619

decryption-failures statement.....1322

default configuration

- NAT.....3
- policies.....3

default configuration file, for autoinstallation.....153

default configuration group.....450

default gateway

- defining (Quick Configuration).....590

delete command.....467

- usage guidelines.....336, 382

Delete Configuration Below This Point option

- button.....608

delete link.....606

deleting

- crash files (J-Web).....934
- files.....970
- files, with caution.....936
- licenses (CLI).....260, 945
- licenses (J-Web).....260, 945
- log files (J-Web).....934
- temporary files (J-Web).....934

deleting a current rescue configuration .....648

deny-commands statement

- usage guidelines.....1062

deny-configuration statement.....782

deny-configuration-regexps statement

- usage guidelines.....1062

denying commands to login classes.....1062

DES encryption

- setting.....932

description statement		
(Security IDP Policy).....	2055	
RMON.....	1902	
usage guidelines (alarms).....	1871	
usage guidelines (events).....	1874	
SNMP.....	1901	
usage guidelines.....	1815	
destination		
NAT.....	43	
Destination Class Usage MIB.....	1735, 1746, 1752	
destination NAT		
configuration.....	43	
verification.....	47	
destination statement		
(Security IP Headers Attack).....	2056	
destination-address statement		
(Security IDP Policy).....	2057	
destination-classes statement.....	1323	
usage guidelines.....	1270	
destination-except statement.....	2058	
destination-interface statement		
RPM.....	1324	
destination-port statement		
(Security Signature Attack).....	2058	
RPM.....	1325	
SNMP.....	1902	
usage guidelines.....	1841	
detect-shellcode statement.....	2059	
detector statement.....	2059	
device		
autoinstallation.....	151	
multiple, deploying <i>See</i> autoinstallation		
packet capture.....	1246	
dfc (system logging facility).....	1642	
DHCP.....	3	
supported software standards.....	2271	
DHCP (Dynamic Host Configuration Protocol)		
autoinstallation, compatibility with.....	687	
conflict detection and resolution.....	688	
interface restrictions.....	689	
monitoring.....	636	
options.....	686	
overview.....	684	
<i>See also</i> DHCP leases; DHCP pages; DHCP		
pools; DHCP server		
server function.....	684	
verification.....	712	
DHCP Local Server		
minimum configuration.....	723, 730	
DHCP server		
preparation.....	685	
sample configuration.....	685	
subnet and single client.....	709, 714, 718	
verifying operation.....	713	
DHCP server, regaining lost lease.....	589, 651	
dhcp-attributes statement IPv4.....	784	
dhcp-attributes statement IPv6.....	786	
dhcp-client attributes.....	727, 735	
dhcp-client statement.....	787	
dhcp-local-server.....	789	
DHCPv6		
configure server options.....	743	
dhcpv6.....	793	
configuring address-assignment pool.....	745	
DHCPv6 client		
identification.....	693	
minimum configuration.....	736	
optional attributes.....	737	
overview.....	693	
TCP/IP propagation.....	741	
DHCPv6 local server		
overview.....	694	
dhcpv6 security policy configuration.....	742	
DHCPv6 server		
preparation.....	743	
dhcpv6-client statement.....	788	
diagnosis		
alarm configurations.....	1278	
CLI command summary.....	1233	
displaying firewall filter for.....	1289	
displaying packet capture		
configurations.....	1284	
interfaces.....	1238, 1358	
J-Web tools overview.....	1233	
license infringement.....	1241	
load balancing on the link services		
interface.....	1622	
monitoring network performance.....	1249	
MPLS connections (J-Web).....	1244	
network traffic.....	1499	
packet capture.....	1246	
packet capture (J-Web).....	1503	
packet encapsulation on link services		
interfaces.....	1621	
ping command.....	1486	
ping host (J-Web).....	1488	
ping MPLS (J-Web).....	1244	
ports.....	1238	

- preparation.....1281
- system logs.....1643
- system operation.....1481
- traceroute (J-Web).....1483
- traffic analysis with packet capture.....1246
- verifying captured packets.....1284
- verifying DHCP server operation.....713
- verifying dialer interfaces.....704
- verifying RPM probe servers.....1300
- verifying RPM statistics.....1297
- VoIP interface.....1627
- diagnostic commands.....1233
- dial-in, USB modem
  - voice not supported.....676
- dial-up modem connection
  - connecting user end.....921
- dialer interface, for USB modem
  - adding (configuration editor).....702
  - See also* USB modem connections
  - verifying.....704
- dialer interface, USB modem
  - limitations.....676
  - naming convention.....676
  - restrictions.....676
- dictionary attacks, preventing.....923
- DiffServ code points, bits for RPM probes.....1306
- direction statement
  - (Security Custom Attack).....2060
  - (Security Dynamic Attack Group).....2061
- directories
  - working, displaying.....531
- disable statement
  - usage guidelines.....389
- disabling
  - console port.....681
  - packet capture.....1292
  - root login to console port.....681
- discard accounting
  - supported software standards.....2310
- Discard All Changes option button.....608
- Discard button.....607
- Discard Changes Below This Point option
  - button.....608
- discarding configuration changes.....607
- disconnection of console cable for console
  - logout.....681
- display detail command
  - usage guidelines.....364
- display inheritance command
  - usage guidelines.....433
- display set command
  - usage guidelines.....361
- display xml filter.....330, 331
- displaying
  - licenses (J-Web).....254, 938
- dl0.....676
- dlv .....872
- DNS name resolution
  - troubleshooting.....1616
- DNS Objects MIB.....1735, 1746, 1752
- DNS server, defining (Quick Configuration).....590
- DNSSEC .....872
- documentation
  - comments on.....lxi
- domain name, defining (Quick Configuration).....589
- domain search, defining (Quick Configuration).....590
- downgrading
  - software, with J-Web.....199
  - software, with the CLI .....199
- downgrading Junos OS.....623
- download URL.....174
- download-timeout statement.....2062
- downloading
  - configuration, with autoinstallation.....153
  - crash files (J-Web).....937
  - licenses (J-Web).....255, 939
  - log files (J-Web).....937
  - software upgrades.....174
  - temporary files (J-Web).....937
- downloading configuration files .....646
- downloading Junos OS.....172
- draft-ietf-vrrp-unified-spec-02.txt.....2305
- drop probabilities, CoS.....1370
- drop profiles, CoS.....1370
- DS1 ports *See* T1 ports
- DS3 ports *See* E3 ports; T3 ports
- DSCPs (DiffServ code points), bits for RPM
  - probes.....1306
- DTCP
  - supported software standards.....2309
- dual-root partitioning.....137
- dual-root partitioning scheme.....145
- DVMRP
  - supported software standards.....2301
- Dynamic Host Configuration Protocol *See* DHCP
- dynamic-attack-group statement.....2063

dynamic-attack-groups (Security IDP).....2064

## E

E3 ports, alarm conditions and configuration  
     options.....1238  
 edit command.....468  
     usage guidelines.....336  
 Edit Configuration page.....605  
 Edit Configuration Text page.....599  
 edit link.....606  
 editing a configuration.....595  
 editing command line.....347  
 egress *See* RPM probes, outbound times  
 Emacs keyboard sequences.....347  
 emergency logging severity.....619  
 enable-all-qmodules statement.....2064  
 enable-packet-pool statement.....2065  
 encapsulation overhead, PPP and MLPPP.....1621  
 encapsulation type  
     verifying for LFI and load balancing.....1621  
 encapsulation, modifying on packet  
     capture-enabled interfaces.....1293  
 encrypted access  
     through HTTPS.....663  
     through SSL.....663  
 engine-id statement  
     SNMPv3.....1903  
     usage guidelines.....1823  
 enterprise-oid statement.....1904  
 enterprise-specific MIBs, listed.....1740, 1745, 1750  
 environment settings, CLI  
     command completion.....511  
     displaying.....511  
     example configuration.....456  
     idle timeout.....511  
     prompt string.....510  
     screen dimensions.....509, 514  
     software upgrade, restarting after.....511  
     terminal type.....510  
     timestamp.....510  
     working directory.....510  
 error logging severity.....619  
 ES-IS  
     supported software standards.....2300  
 ESO Consortium standards supported *See* Index of  
     Supported Software Standards  
 Ethernet interfaces  
     supported software standards.....2284  
 Ethernet MAC MIB.....1741, 1747, 1752

Ethernet ports  
     alarm conditions and configuration  
         options.....1238  
     autoinstallation on.....152  
     configuring alarms on.....1276  
 Ethernet rollover cable, connecting the router to a  
     management device.....1612  
 Event MIB.....1735, 1741, 1747, 1753  
 event options, configuration summary.....596  
 event statement.....1904  
     usage guidelines.....1874  
 event viewer, J-Web  
     overview.....1378, 1696  
     *See also* system log messages  
 event-rate statement.....1672  
 events  
     filtering.....619  
     filters.....619  
     overview.....617  
     regular expressions for filtering.....621  
     severity levels.....619  
     using.....617  
     viewing.....618  
     viewing, sample.....622  
 events sample task.....622  
 except command.....533  
 except filter.....331  
 exclude statement.....1674  
 exit command.....469  
     from configuration mode.....371  
     usage guidelines.....336, 359  
 exit configuration-mode command.....469  
     usage guidelines.....359  
 explicit-priority statement.....1673  
     usage guidelines  
         single-chassis system.....1662  
 expression statement.....2065  
 extension command  
     usage guidelines.....336

## F

facilities (system logging)  
     default for remote machine.....1660  
     for local machine.....1642  
 facility-override statement.....1675  
 factory default configuration.....3  
 falling-event-index statement.....1905  
     usage guidelines.....1871

- falling-threshold statement
  - health monitor.....1906
  - usage guidelines.....1877
  - RMON.....1907
- falling-threshold-interval statement
  - RMON.....1908
  - usage guidelines.....1872
- false-positives statement.....2066
- family statement.....797
- FAQ (frequently asked questions)
  - Are LFI and load balancing working correctly?.....1618
  - What causes jitter and latency on multilink bundles?.....1618
  - Which CoS components apply on link services interface?.....1617
  - Why Are Packets Dropped on a PVC Between a J Series Device and Another Vendor?.....1625
  - Why is the VoIP interface unavailable?.....1627
- fe-0/0/0, defining address (Quick Configuration).....591
- feature licenses See license See licenses
- fields statement
  - for interface profiles.....1326
  - usage guidelines.....1261
  - for Routing Engine profiles.....1327
  - usage guidelines.....1275
- file See security log
- file archive command.....960
- file checksum md5 command.....962
- file checksum sha-256 command.....964
- file checksum sha1 command.....963
- file command.....543
- usage guidelines.....320, 497, 512, 513
- file compare command.....965
- file copy command.....968
- file delete command.....970
- file encryption
  - decrypting configuration files.....932
  - encrypting configuration files.....932
- file list command.....971
- file management
  - configuration files.....695
  - crash files .....649
  - crash files (CLI).....935
  - crash files (J-Web).....934
  - log files .....649, 695
  - log files (CLI).....935
  - log files (J-Web).....934
  - packet capture file creation.....1247
  - temporary files .....649
  - temporary files (CLI).....935
  - temporary files (J-Web).....934
- file rename command.....972
- file show command.....973
- file statement
  - accounting (associating with profile).....1328
  - usage guidelines (filter profile).....1264
  - usage guidelines (interface profile).....1261
  - usage guidelines (MIB profile).....1273
  - usage guidelines (Routing Engine profile).....1275
  - accounting (configuring log file).....1329
  - usage guidelines.....1257
  - system logging.....1677
  - usage guidelines.....1658
- filenames, specifying in commands.....500
- files
  - archiving.....960
  - calculating checksum.....962, 963, 964
  - comparing.....965
  - compressing.....960
  - contents, displaying.....973
  - copying.....968
  - deleting.....970
  - list of, displaying.....971
  - listing.....498
  - log file, clearing.....1699
  - renaming.....972
  - saving command output to.....334
  - saving configurations to files.....573
  - status of, displaying.....1512, 1703
  - viewing.....497
- files statement.....1330, 1678
- archiving of all system log files.....1669
- filter profile.....1263
- filter-duplicates statement.....1908
- usage guidelines.....1819
- filter-interfaces statement.....1909
- filter-profile statement.....1330
- usage guidelines.....1263
- filtering
  - command output.....1231
- filtering events
  - overview.....619
  - regular expressions.....621
- filtering get SNMP requests.....1819

filters statement.....	2067
find command.....	533
find filter.....	331
firewall.....	7
firewall (system logging facility).....	1642
firewall filters	
configuration summary.....	596
for packet capture, configuring.....	1287
for packet capture, overview.....	1247
monitoring.....	634
sample task.....	622
statistics	
displaying.....	118, 124, 1050
Firewall MIB.....	1736, 1741, 1747, 1753
flags	
login class.....	1059, 1064
user permissions.....	1059
flow monitoring	
supported software standards.....	2310
flow statement	
(Security Flow).....	1331
(Security IDP).....	2068
font conventions.....	lix
forwarding classes, CoS.....	1371
Forwarding Engine Board redundancy	
monitoring.....	638
forwarding options, configuration summary.....	596
forwarding-options statement.....	798
fragmentation, verifying on the link services	
interface.....	1620
Frame Relay interfaces	
supported software standards.....	2285
FreeBSD UNIX kernel.....	310
frequency, test See RPM probes, test intervals	
FRF (Broadband Forum) standards supported See	
Index of Supported Software Standards	
from-zone statement	
(Security IDP Policy).....	2068
ftp (system logging facility).....	1642
fxp0, defining address (Quick Configuration).....	591

## G

ge-0/0/0, defining address (Quick	
Configuration).....	591
Get requests, SNMP.....	1716
GMPLS	
supported software standards.....	2291
GR (Generic Requirements) standards supported	
See Index of Supported Software Standards	

GRE interfaces	
supported software standards.....	2286
group licenses.....	158, 697
group statement.....	799
SNMPv3 (for access privileges).....	1911
usage guidelines.....	1834
SNMPv3 (for configuring).....	1910
usage guidelines.....	1854
group-members statement.....	2070
groups	
BGP, displaying.....	1419
Groups Configuration Statement Hierarchy.....	768
groups statement.....	463
usage guidelines.....	428
when.....	491

## H

halting a Services Router immediately.....	627
hard disk.....	135
hardware	
major (red) alarm conditions on.....	616, 1237
timestamp See RPM probe timestamps	
hardware architecture overview	
J Series routers.....	134
hardware, major (red) alarm conditions	
on.....	616, 1237
hardware-timestamp statement.....	1333
header-length statement.....	2071
health-monitor statement.....	1911
usage guidelines.....	1877
heat status, checking.....	1448
help apropos command	
usage guidelines.....	316
help command.....	470, 544
usage guidelines.....	316, 336
Help icon (?).....	582, 584
help reference command	
usage guidelines.....	316
help syslog command	
usage guidelines.....	1635
help tip cli command	
usage guidelines.....	318
Help, J-Web interface.....	580, 584
history, CLI commands	
displaying.....	532
operational mode.....	455
hold command.....	533
hold filter.....	332
host (Security Logging) statement.....	1679

- 
- host reachability
    - ping command.....1486
    - ping host (J-Web).....1488
  - Host Resources MIB.....1736, 1741, 1747, 1753
  - host statement
    - (Security IDP Sensor Configuration).....2071
    - ssh-known-hosts.....802
  - host-specific configuration file, for
    - autoinstallation.....153
  - hostkey-algorithm.....803
  - hostname.....18, 26
    - monitoring traffic by matching.....1501
    - opening an SSH session to.....929
    - pinging (CLI).....1486
    - pinging (J-Web).....1488
    - resolving.....685
    - telnetting to.....928
    - tracing a route to (CLI).....1360, 1480
    - tracing a route to (J-Web).....1483
  - hostname, defining (Quick Configuration).....589
  - hostname.conf file, for autoinstallation.....153, 205
  - hosts, reachability
    - MPLS Layer 2 circuits.....1531
    - MPLS Layer 2 VPN connections.....1528
    - MPLS Layer 3 VPN connections.....1534
    - MPLS LDP LSPs.....1536
    - MPLS LSP endpoints.....1539
    - MPLS RSVP LSPs.....1541
  - HTTP (Hypertext Transfer Protocol)
    - enabling Web access.....612, 890
    - enabling Web access (configuration editor).....892
    - on built-in management interfaces.....591, 663
    - verifying configuration.....893
  - HTTP (Hypertext Transfer Protocol), RPM probes.....1249
  - httpd process, limiting subordinate processes.....611
  - HTTPS (Hypertext Transfer Protocol over SSL)
    - enabling secure access.....612, 890
    - enabling secure access (configuration editor).....892
    - J-Web configuration.....890
    - recommended for secure access.....591, 663
    - verifying secure access configuration.....893
  - HTTPS Web access, establishing.....663
  - Hypertext Transfer Protocol See HTTP
  - Hypertext Transfer Protocol over SSL See HTTPS
  - Hypertext Transfer Protocol, RPM probes.....1249
- I**
- IANA standards supported See Index of Supported Software Standards
  - ICMP
    - supported software standards.....2300
  - ICMP (Internet Control Message Protocol)
    - RPM probes, description.....1249
    - RPM probes, inbound and outbound times.....1250
    - RPM probes, setting.....1294
  - icmp statement
    - (Security IDP Custom Attack).....2072
    - (Security IDP Signature Attack).....2073
  - icmpv6 (Security IDP).....2074
  - identification statement
    - (Security ICMP Headers).....2074
    - (Security IP Headers).....2075
  - identifier link.....606
  - identifiers
    - inserting in sequential lists.....386
    - renaming.....385
    - specifying.....344
  - idle timeout
    - user, setting.....520
    - values, CLI sessions.....511
  - IDP.....12
    - configuration.....53
    - log suppression.....1995
    - logging, overview.....1995
    - maximize-idp-sessions.....1998
    - packet capture.....1998
    - performance and capacity tuning.....1998
    - recommended
      - policy.....12
      - send attack logs to the IC.....1997
      - template.....12
      - verification.....56
  - IDP MIB.....1736, 1744
  - idp potential violation statement.....1333, 2076
  - idp statement
    - (Security Policies).....2075
  - idp-policy statement.....2077
  - IEEE standards supported See Index of Supported Software Standards
  - IGMP
    - supported software standards.....2301
  - ignore filter.....331
  - ignore-memory-overflow statement.....2079
  - ignore-reassembly-overflow statement.....2080



ignore-regular-expression statement.....	2080	interface-traceoptions statement	
IKE		DHCP local server.....	807
supported software standards.....	2310	interfaces See management interfaces; network	
ILMI.....	1801	interfaces; ports	
inbound time See RPM probes		configuration summary.....	596
INCITS standards supported See Index of Supported		media parameters.....	442, 444
Software Standards		monitoring.....	630
include-destination-address statement.....	2081	interfaces (ARP).....	805
info logging severity.....	619	interfaces (autoinstallation).....	248
informs SNMP See SNMP informs		Interfaces Configuration Statement Hierarchy.....	753
ingress See RPM probes, inbound times		interfaces limiting SNMP access.....	1820
inheritance model, configuration groups.....	354	interfaces statement.....	806
inherited values, configuration groups.....	433	internet.....	18, 27
init-command-string command.....	678	Internet drafts supported See Index of Supported	
initial configuration requirements.....	588	Software Standards	
insert command.....	471	Internet Explorer, modifying for worldwide version	
usage guidelines.....	336, 386	of Junos OS.....	587, 666
install.....	2081	internet service provider (isp).....	15
Install Remote page		interval statement	
field summary.....	186, 193	(Security IDP).....	2082
installation		accounting.....	1335
licenses (CLI).....	257, 941	usage guidelines (filter profile).....	1264
licenses (J-Web).....	257, 941	usage guidelines (interface profile).....	1261
memory requirements		usage guidelines (MIB profile).....	1273
J Series routers.....	134	usage guidelines (Routing Engine	
software upgrades (CLI).....	177	profile).....	1275
software upgrades, from a remote server.....	185	health monitor.....	1913
software upgrades, uploading.....	177	usage guidelines.....	1878
installation modules.....	142	RMON.....	1912
installation types.....	136	usage guidelines.....	1872
installing Junos OS.....	623	intervals, probe and test See RPM probes	
Instance to which this connection belongs		intrusion detection and prevention.....	12
description.....	1244	invalid configuration, replacing.....	648
using.....	1491	IP Forward MIB.....	1736, 1742, 1747, 1753
integrated local management interface See ILMI		IP multicast	
interactive-commands (system logging		supported software standards.....	2301
facility).....	1642	tracing routes	
interface		listen for responses.....	1526
configuration example.....	374	ip statement	
Interface MIB.....	1736, 1742, 1747, 1753	(Security IDP Custom Attack).....	2082
interface names		ip-action statement	
conventions.....	493	(Security Application-Level DDoS).....	2083
interface profile.....	1260	(Security IDP Rulebase IPS).....	2084
interface statement.....	804	ip-block statement.....	2085
SNMP.....	1912	ip-close statement.....	2085
usage guidelines.....	1820	ip-connection-rate-limit statement.....	2086
interface-profile statement.....	1334	ip-flags statement.....	2087
usage guidelines.....	1260	IP-IP interfaces	
		supported software standards.....	2286



- 
- ip-notify statement.....2087
  - ipconfig command.....713
    - explanation.....713
  - ips statement.....2088
  - IPsec.....12
    - supported software standards.....2310
  - IPsec Generic Flow Monitoring Object
    - MIB.....1736, 1742, 1748, 1753
  - IPsec Monitoring MIB.....1736, 1742, 1747, 1753
  - IPsec tunnels
    - monitoring.....635
  - IPsec VPN Objects MIB.....1737
  - IPv4
    - supported software standards.....2302
  - IPv4 MIB.....1737, 1742, 1748, 1754
  - ipv4 statement
    - (Security IDP Signature Attack).....2089
  - IPv6
    - supported software standards.....2303
  - ipv6 (Security IDP).....2090
  - IPv6 and ICMPv6 MIB.....1737
  - IPv6 SNMP community string.....1862
  - IS-IS
    - supported software standards.....2306
  - ISO/IEC standards supported See Index of Supported Software Standards
  - issuing relative configuration commands.....385
  - ITU–T Recommendations supported See Index of Supported Software Standards
- J**
- J Series.....695
    - alarms.....1237
    - licenses.....157, 696
    - managing user authentication.....671
    - monitoring .....1231
    - packet capture.....1246
    - performance monitoring.....1249
    - system log messages.....1643
    - user interfaces See user interfaces
  - J series
    - install remote page
      - field summary.....187
  - J series device
    - boot devices.....213
      - storing memory snapshots.....208
    - See also CompactFlash card
    - bring components online/offline.....271
  - chassis-control
    - restart options.....266
  - compactFlash.....138
  - CompactFlash card
    - configuring.....213
      - configuring for failure snapshot storage.....208
  - configuration
    - downgrading software (CLI).....201
    - upgrading (CLI).....179
  - configuration, downgrading software (J-Web).....201
  - device
    - halting (J-Web).....263
  - downgrading
    - software, with the CLI .....201
  - downgrading software ( J-Web).....201
  - downloading.....175
  - halting (CLI).....268
  - halting a
    - with J-Web.....263
  - installation
    - software upgrades (CLI).....179
    - software upgrades, from a remote server.....186
  - installing by uploading.....179
  - internal CompactFlash card See CompactFlash card
  - rebooting
    - with J-Web .....263
  - rebooting (CLI).....263
  - request system halt command.....268
  - request system reboot command.....263
  - request system snapshot command.....213
    - options.....213
  - reverting to a previous configuration file (J-Web).....201
  - rolling back a configuration file.....201
  - snapshots
    - configuring for failure snapshot storage.....208
  - software.....138
  - software upgrades.....138, 175
  - software upgrades, uploading.....179
  - storage media
    - configuring boot devices.....213
  - upgrades
    - installing (CLI).....179
    - installing from remote server.....186

upgrades requirements.....	167	unpredictable results, multiple windows.....	651
upgrading.....	138	windows, multiple, unpredictable results	
USB		with.....	671
configuring.....	213	J-Web Quick Configuration See Quick Configuration	
configuring for failure snapshot		J-Web software, installing.....	585
storage.....	208	jitter	
J series device boot devices		description.....	1250
configuring (CLI).....	213	<i>See also</i> RPM probes	
configuring (J-Web).....	213	in RPM probes, improving with	
J-web.....	6	timestamps.....	1250
J-Web Configuration		monitoring.....	1507
secure Web access.....	890	threshold, setting.....	1306
J-Web configuration		jitter, removing on multilink bundles.....	1618
adding users.....	902	jnxRmonAlarmTable.....	1805
authentication method.....	900	Juniper Networks MIB objects.....	1766
J-Web configuration editor		juniper-ais configuration group	
autoinstallation.....	205	usage guidelines.....	428
committing a configuration.....	607	Junos OS	
configuration hierarchy display.....	583	autoinstallation.....	151
configuration text, viewing.....	597	downgrading.....	623
controlling user access.....	902	downloading.....	172
editing a configuration.....	604	editions.....	130
interface alarms.....	1276	Canada and U.S.....	130
RADIUS authentication.....	895	Junos-FIPS.....	131
RPM.....	1294	worldwide.....	131
secure access.....	892	generating licenses.....	254, 939
system log messages, sending to a file.....	1652	information security.....	137
TACACS+ authentication.....	897	installation	
J-Web graphical user interface (GUI).....	314	current configuration, confirming.....	175
J-Web interface		installation modules.....	142
comparing configuration differences.....	646	installing.....	623
context-sensitive help.....	580	Internet Explorer, modifying for worldwide	
Diagnose options.....	1233	version.....	587, 666
event viewer.....	622, 1378, 1696	introduction.....	129
Help (?) icon.....	582	naming convention.....	131
Internet Explorer, modifying for worldwide		packages	
version of Junos OS.....	587, 666	digital signatures.....	137
layout.....	580	MD5 checksum.....	137
losing connectivity after initial		naming conventions.....	132
configuration.....	651	SHA-1 checksum.....	137
main pane.....	581	release naming conventions.....	132
managing licenses.....	157, 697	release numbers.....	132
overview.....	579, 593, 665	software installation types.....	136
page layout.....	580, 667	storage media.....	135
sessions.....	671	device names.....	135
side pane.....	582	upgrading.....	137, 623
starting.....	586, 666	version, displaying.....	170
top pane.....	580	worldwide version, modifying Internet Explorer	
		for.....	587, 666

- 
- Junos OS CLI.....601
    - access privilege levels.....673
    - command modes.....602, 666
    - denying and allowing commands.....675
    - diagnostic command summary.....1234
    - filtering command output.....1231
    - overview.....601, 666
    - See also CLI terminal
  - Junos OS versions See Junos OS editions
  - Junos Scope application.....664
  - Junos XML management protocol.....314
    - enabling secure access.....890
    - verifying secure access configuration.....893
  - Junos XML protocol over SSL.....890
  - junos-defaults configuration group.....566
    - displaying.....450, 562, 566
  - Junos-FIPS software environment.....314
  - JUNOScript
    - enabling secure access.....612
  - JUNOScript API
    - defining access (Quick Configuration).....591
  - JUNOScript over SSL.....612
  - K**
  - kernel (system logging facility).....1642
  - key performance indicators.....1808
  - key-protection statement
    - (Security IDP Sensor Configuration).....2090
  - keyboard sequences
    - editing command line.....347
  - L**
  - L2TP
    - supported software standards.....2289, 2311
  - label-switched paths See LSPs
  - LAN.....3
  - laptop See management device
  - last command.....533
  - last filter.....332
  - latency, in RPM probes, improving with
    - timestamps.....1250
  - latency, reducing on multilink bundles.....1618
  - Layer 2 circuits
    - reachability, testing.....1531
    - supported software standards.....2290
  - Layer 2 circuits, monitoring.....1244
  - Layer 2 networking
    - supported software standards.....2289
  - Layer 2 VPNs
    - reachability, testing.....1528
  - Layer 2 VPNs, monitoring.....1244
  - Layer 3 VPNs
    - reachability, testing.....1534
  - Layer 3 VPNs, monitoring.....1244
  - layout, J-Web.....580
  - LDP
    - supported software standards.....2292
  - LDP LSPs
    - ping interval.....1536
  - lease-time (dhcp-client) statement.....810
  - libpcap format, for packet capture files.....1284
  - license
    - add.....624
    - advanced BGP feature.....624
    - delete.....624
    - display keys.....624
    - manage.....624
  - license infringement
    - identifying any licenses needed.....158, 697
    - verifying license usage.....259, 944
    - verifying licenses installed.....259, 261, 944, 946
  - license keys
    - components.....157, 696
    - displaying (CLI).....259, 944
    - status.....158, 697
    - version.....158, 697
  - License MIB.....1737, 1742, 1748, 1754
  - licenses.....48
    - adding (CLI).....257, 941
    - adding (J-Web).....257, 941
    - deleting (CLI).....260, 945
    - deleting (J-Web).....260, 945
    - displaying.....121, 298, 1046
    - displaying (CLI).....259, 261, 944, 946
    - displaying (J-Web).....157, 254, 697, 938
    - displaying usage.....259, 944
    - downloading (J-Web).....255, 939
    - generating.....254, 939
    - group.....158, 697
    - infringement, preventing.....157, 697
    - See also license infringement
    - key.....157, 696
    - See also license keys
    - managing (J-Web).....157, 697
    - overview.....157, 696
    - saving (CLI).....255, 940

updating (CLI).....	256, 941
verifying.....	259, 261, 943, 946
licenses, alarm conditions and remedies.....	1241
limit statement	
cache	
security log.....	1679
limitations	
ALARM LED lights yellow whether alarm is	
minor or major.....	1237
DHCP, no support on VPN interfaces.....	689
MPLS, no LSP statistics on outbound	
device.....	1388
mtrace from-source packet statistics always	
O.....	1356
performance degradation with monitor traffic	
command.....	1499
PPP, no J-Web monitoring information	
available.....	1403
Server relay and DHCP client cannot coexist in	
device.....	684
software downgrade cannot be	
undone.....	199, 624
unpredictable behavior with multiple	
windows.....	651
link services	
supported software standards.....	2311
link services interface	
applying CoS components on constituent	
links.....	1617
fragmentation, troubleshooting.....	1620
load balancing, troubleshooting.....	1622
MLPPP header overhead.....	1621
packet encapsulation, troubleshooting.....	1621
PPP header overhead.....	1621
preventing dropped packets on PVCs.....	1625
reducing jitter and latency on multilink	
bundles.....	1618
troubleshooting LFI and load balancing.....	1618
load balancing on link services interfaces	
FAQ.....	1618
troubleshooting.....	1618
verifying.....	1622
load command.....	472
usage guidelines.....	336
load merge command	
usage guidelines.....	422
load override command	
usage guidelines.....	422
load set command	
usage guidelines.....	423
loading a configuration file	
downloading .....	646
rollback .....	645
uploading .....	647
local password	
default authentication method for	
system.....	900
method for user authentication .....	900
order of user authentication (configuration	
editor).....	900
overview.....	671, 672
local template accounts.....	908
local-engine statement.....	1914
Locate LSP from interface name	
description.....	1244
using.....	1491
Locate LSP from virtual circuit information	
description.....	1244
using.....	1491
Locate LSP using interface name	
description.....	1244
using.....	1491
location statement	
SNMP.....	1915
usage guidelines.....	1816
locking configuration.....	367
lockout-period statement.....	811
log.....	1700
Services .....	1680
log file.....	1702
log files	
archiving.....	695
clearing contents of.....	1699
contents, displaying.....	1707
deleting unused files.....	695
display of	
starting.....	1513, 1704
stopping.....	1515, 1706
rotating.....	695
status, displaying.....	1512, 1703
log messages See system log messages	
log statement	
(Security IDP Policy).....	2091
(Security IDP).....	2091
log suppression.....	1995
configuring.....	1996
log-attacks statement.....	2092

- log-create statement.....2092
- log-errors statement.....2093
- log-prefix statement
  - system logging.....1681
  - usage guidelines.....1661
- log-rotate-frequency statement.....1681
- log-supercede-min statement.....2093
- logging
  - IDP, overview.....1995
- logging severity levels.....619
- logical interfaces
  - unit numbers.....494
- logical interfaces, CoS.....1367
- logical operators
  - for monitor traffic command.....1519
- logical operators, for multicast traffic.....1502
- Logical Systems MIB.....1737, 1748, 1754
- logical-system statement.....1916
- logical-system-trap-filter statement.....1917
- login classes
  - access privilege levels.....1059
  - commands, allowing or denying.....1062
  - defining.....1063
  - defining (configuration editor).....902
  - permission bits for.....674
  - predefined permissions.....673
  - specifying.....902
- login lockout.....301, 959, 1049
- login retry limits, setting.....923
- login statement
  - usage guidelines.....1063
- logs See system logs
- loopback address, defining (Quick Configuration).....590
- loss priority, CoS.....1373
- LSPs
  - LDP, ping interval.....1536
  - RSVP, ping interval.....1541
- LSPs (label-switched paths)
  - information about.....1388
  - monitoring, with ping MPLS.....1244
  - statistics.....1389
- LSYS MIB.....1737
- M**
- macs.....875
- main pane, J-Web.....581
- major (red) alarms.....616
  - description.....1237
- Management Access page
  - description.....613
- management device
  - connecting through the CLI.....1612
  - connecting to console port.....1612
  - diagnosing problems from.....1232
  - monitoring from.....628, 1231
  - recovering root password from.....1612, 1614
- Management Information Base See MIBs
- management interface address, defining (Quick Configuration).....591
- management interfaces
  - alarm conditions and configuration
    - options.....1238
  - configuring alarms on.....1276
  - monitoring.....1358, 1382
  - statistics.....1358
- managing
  - files.....695
  - software.....137
  - user authentication.....671
- manuals
  - comments on.....lxi
- master agent, SNMP.....1718
- match command.....533
- match conditions
  - for monitor traffic command.....1518
- match conditions, for multicast traffic
  - .....1501
- match filter.....332
- match statement.....1682
  - (Security IDP Policy).....2094
  - (Security Rulebase DDoS).....2095
  - usage guidelines.....1664
- max-flow-mem statement.....2095
- max-logs-operate statement.....2096
- max-packet-mem-ratio statement.....2096
- max-packet-memory-ratio statement.....2097
- max-reass-packet-memory-ratio
  - statement.....2097
- max-sessions statement
  - (Security Packet Log).....2098
- max-tcp-session-packet-memory
  - statement.....2098
- max-time-report statement.....2099
- max-timers-poll-ticks statement.....2099
- max-udp-session-packet-memory
  - statement.....2100
- maximum-aggregate-pool statement.....473

maximum-capture-size	
security log.....	1336
maximum-entries statement.....	474
MD5 (Message Digest 5) checksum.....	137
MD5 checksum, calculating.....	962
member statement	
(Security IDP).....	2100
memory requirements	
J Series routers.....	134
message-processing-model statement.....	1917
usage guidelines.....	1850
messages See system log messages	
broadcast messages, NTP.....	779
MIB profile.....	1272
mib-profile statement.....	1336
usage guidelines.....	1272
MIBs	
AAA Objects.....	1733, 1745, 1751
Access Authentication	
Objects.....	1733, 1740, 1745, 1751
Alarm.....	1733, 1740, 1745, 1751
ATM.....	1734
ATM CoS.....	1734, 1745, 1751
BFD.....	1734, 1741, 1746, 1751
BGP4 V2.....	1734, 1740, 1745, 1751
Chassis.....	1734, 1741, 1746, 1752
Chassis Cluster.....	1735, 1746, 1752
Chassis Definitions for Router Model.....	1734
Chassis Forwarding.....	1734
Class-of-Service.....	1735
Configuration	
Management.....	1735, 1741, 1746, 1752
Destination Class Usage.....	1735, 1746, 1752
DNS Objects.....	1735, 1746, 1752
enterprise-specific, listed.....	1740, 1745, 1750
Ethernet MAC.....	1741, 1747, 1752
Event.....	1735, 1741, 1747, 1753
Firewall.....	1736, 1741, 1747, 1753
Host Resources.....	1736, 1741, 1747, 1753
IDP.....	1736
Interface.....	1736, 1742, 1747, 1753
IP Forward.....	1736, 1742, 1747, 1753
IPsec Generic Flow Monitoring Object	
.....	1736, 1742, 1748, 1753
IPsec Monitoring.....	1736, 1742, 1747, 1753
IPsec VPN Objects.....	1737
IPv4.....	1737, 1742, 1748, 1754
IPv6 and ICMPv6.....	1737
License.....	1737, 1748
license.....	1742, 1754
Logical Systems.....	1737
logical systems.....	1748, 1754
LSYS.....	1737
Multicast.....	1725, 1733
NAT Objects.....	1737, 1743, 1748, 1754
OSPF.....	1722
Packet Forwarding	
Engine.....	1737, 1743, 1748, 1754
Ping.....	1738, 1743, 1748, 1754
use in ping test.....	1966
view configuration example, SNMP.....	1822
Policy Objects.....	1738, 1743, 1748, 1754
PPP.....	1721
Reverse-Path-Forwarding.....	1738, 1743, 1749, 1754
RMON Events and Alarms	
.....	1738, 1743, 1749, 1755
Security Interface Extension	
Objects.....	1738, 1743, 1749, 1755
Security Screening Objects.....	1738, 1749, 1755
SNMP IDP.....	1736, 1744
SNMP object values, displaying.....	1991
Source Class Usage.....	1739, 1749, 1755
SPU Monitoring.....	1739, 1749
SPU monitoring.....	1755
Structure of Management	
Information.....	1739, 1740, 1745
Junos OS for J Series and SRX Series	
devices, for.....	1740, 1745, 1751
System Log.....	1739, 1744, 1750, 1755
Traceroute.....	1739, 1744, 1750, 1756
Utility.....	1739, 1744, 1750, 1756
views	
SNMP.....	1821
VPN.....	1740
VPN Certificate Objects.....	1739, 1744, 1750, 1756
minimum accounting options configuration.....	1256
minor (yellow) alarms.....	616
description.....	1237
MLD	
supported software standards.....	2301
MLPPP encapsulation, on the link services	
interface.....	1621
Mobile IP	
supported software standards.....	2272
mode (Security Logging) statement.....	1682
modem connection to router USB port	
connecting USB modem to router.....	679

- 
- monitor interface command.....1358
    - controlling output.....1358
  - monitor interface traffic command.....1358
    - controlling output.....1359
  - monitor list command.....1481, 1512, 1703
  - monitor sample task.....638, 640
  - monitor start command.....1481, 1513, 1704
  - monitor stop command.....1481, 1515, 1706
  - monitor traffic command.....1499, 1516
    - options.....1499
    - performance impact.....1499
  - monitor traffic matching command.....1499
    - arithmetic, binary, and relational operators.....1503
    - logical operators.....1502
    - match conditions.....1501
  - monitoring
    - BGP.....1419
    - BGP neighbors, with RPM probes.....1301
    - chassis.....637, 1448
    - chassis viewer.....628
    - class of service.....629
    - CLI commands and corresponding J-Web options.....628
    - DHCP.....636
    - FEB redundancy.....638
    - firewall filters.....634
    - interfaces.....630, 1358, 1382
    - interfaces, sample.....638
    - IPsec.....635
    - J-Web tasks and corresponding CLI commands.....628
    - Layer 2 circuits.....1244
    - Layer 2 VPNs.....1244
    - Layer 3 VPNs.....1244
    - MPLS.....631
    - MPLS traffic
      - engineering.....1387, 1388, 1389, 1391
    - NAT.....635
    - network interface traffic.....1499
    - network traffic with packet capture.....1246
    - OSPF.....1417
    - overview.....628
      - See also* diagnosis; statistics; status
    - ports.....1382
    - PPP (CLI).....1403
    - PPPoE.....632, 1404
    - preparation.....1281
    - Process Details.....637
    - RIP.....1416
    - route information, sample.....640
    - routing.....633
    - routing information.....1413
    - routing tables.....1414
    - RPM.....632
    - RPM probes.....1507
    - service quality.....1807
    - service sets.....636
    - system.....637
    - system log messages.....1643
    - system logs.....1481
    - trace files.....1481
  - monitoring the wx interface.....1476
  - MPLS
    - Layer 2 circuit connections
      - operability, checking.....1531
    - Layer 2 VPN connections
      - operability, checking.....1528
    - Layer 3 VPN connections
      - operability, checking.....1534
    - LDP-signaled LSP connections
      - operability, checking.....1536
    - LSP endpoint connections
      - operability, checking.....1539
    - standard traps.....1792
    - supported software standards.....2293
  - MPLS (Multiprotocol Label Switching)
    - connections, checking.....1244
    - LSPs.....1388
    - monitoring interfaces.....1387
    - monitoring LSP information.....1387
    - monitoring LSP statistics.....1388, 1389
    - monitoring MPLS interfaces.....1387
    - monitoring RSVP interfaces.....1391
    - monitoring RSVP sessions.....1389
    - monitoring traffic engineering.....1387
  - mpls statement.....1337
  - MPLS, monitoring.....631
  - MSDP
    - supported software standards.....2301
  - mss statement
    - (Security IDP).....2101
  - mtrace monitor command.....1482, 1526
    - results.....1482
  - mtrace-from-source command.....1356
    - options.....1356
    - results.....1357



multicast	
trace operations, displaying.....	1482
tracing paths.....	1356
Multicast MIB.....	1725, 1733
multicast-client statement.....	811
multilink bundles	
preventing dropped packets.....	1625
reducing latency.....	1618
removing jitter.....	1618
multiple devices	
deploying See autoinstallation	
Multiprotocol Label Switching See MPLS	
<b>N</b>	
name statement.....	1918
usage guidelines.....	1816
names	
wildcard .....	448
naming conventions, interface.....	493
naming conventions, software.....	131
NAT	
supported software standards.....	2312
NAT (Network Address Translation)	
monitoring.....	635
NAT Objects MIB.....	1737, 1743, 1748, 1754
negate statement.....	2101
neighbor discovery	
supported software standards.....	2300
neighbor-discovery-router-advertisement	
statement.....	812
neighbors, BGP See BGP neighbors; BGP RPM	
probes	
nested configuration groups.....	430
nested-application (Security IDP).....	2102
network address translation.....	9
Network Address Translation See NAT	
Network Address Translation Objects MIB See NAT	
Objects MIB	
network connectivity.....	653
network interfaces	
alarm conditions and configuration	
options.....	1238
configuring alarms on.....	1276
integrated services, alarm conditions and	
configuration options.....	1238
monitoring.....	1358, 1382
monitoring MPLS traffic engineering.....	1387
monitoring traffic.....	1499
monitoring, CoS.....	1367
monitoring, PPPoE.....	1404
monitoring, RSVP.....	1391
packet capture, configuring on.....	1286
packet capture, disabling before changing	
encapsulation.....	1293
packet capture, supported on.....	1247
services, alarm conditions and configuration	
options.....	1238
statistics.....	1358
network management	
supported software standards.....	2273
network performance See RPM	
network.conf file, default for	
autoinstallation.....	153, 205
next hop, displaying.....	1415
no-allow-icmp-without-flow statement.....	2022
no-detect-shellcode statement.....	2059
no-enable-all-qmodules statement.....	2064
no-enable-packet-pool statement.....	2065
no-ignore-memory-overflow statement.....	2079
no-ignore-regular-expression statement.....	2080
no-include-destination-address statement.....	2081
no-log-errors statement.....	2093
no-more command.....	533, 534
no-more filter.....	333
no-policy-lookup-cache statement.....	2106
no-process-ignore-s2c statement.....	2110
no-process-override statement.....	2110
no-reset-on-policy statement.....	2121
no-world-readable statement	
archiving of all system log files.....	1669
system logging.....	1696
nonpersistent statement.....	1338
accounting	
usage guidelines.....	1258
Nontemporary Address	
configuring.....	738
Nontemporary Addresses and Prefix	
Delegation.....	739
nonvolatile statement.....	1918
notice logging severity.....	619
notification statement.....	2102
notify statement.....	1919
usage guidelines.....	1845
notify-filter statement	
for applying to target.....	1919
usage guidelines.....	1850
for configuring.....	1920
usage guidelines.....	1840



- notify-view statement.....1920
  - usage guidelines.....1856
- NTP
  - listening
    - for broadcast messages.....779
    - supported software standards.....2283
  - ntp server.....23, 31
  - NTP server, defining (Quick Configuration).....590
  - ntp statement.....813
- O**
  - object-names statement.....1338
  - objects-names statement
    - for Routing Engine profiles
      - usage guidelines.....1273
  - oid statement
    - SNMP.....1921
      - usage guidelines.....1821
    - SNMPv3.....1921
      - usage guidelines.....1840
  - OK button.....607
    - J-Web configuration editor.....584
  - Open Shortest Path First See OSPF
  - openssl command.....592, 888
  - operation statement.....1339
    - for MIB profiles
      - usage guidelines.....1273
  - operational mode, CLI
    - command history.....455
    - switching to configuration mode.....370
    - users, monitoring.....497
    - word history.....455
  - operational mode, filtering command output.....1231
  - operator login class permissions.....673
  - operators
    - arithmetic, binary, and relational
      - operators.....1503
    - logical.....1502
  - operators, regular expression
    - system logging.....1665
  - option buttons
    - Delete Configuration Below This Point.....608
    - Discard All Changes.....608
    - Discard Changes Below This Point.....608
  - option statement
    - (Security IDP).....2103
  - order statement
    - (Security IDP).....2103
  - OSPF
    - supported software standards.....2307
  - OSPF (Open Shortest Path First)
    - monitoring.....1417
    - statistics.....1417
  - OSPF interfaces
    - displaying.....1417
    - status.....1417
  - OSPF MIB.....1722
  - OSPF neighbors
    - displaying.....1417
    - status.....1417
  - OSPF routing information.....1417
  - OSPFv3
    - supported software standards.....2307
  - outbound time See RPM probes
  - overrides statement
    - DHCP local server.....814
  - overview
    - branch SRX.....3
- P**
  - P2MP LSPs, testing.....1541
  - packet capture.....656
    - configuring.....1286
    - configuring (J-Web).....1503
    - configuring on an interface.....1286
    - device interfaces supported.....1247
    - disabling.....1292
    - disabling before changing encapsulation on
      - interfaces.....1293
    - displaying configurations.....1284
    - displaying firewall filter for.....1289
    - enabling.....1282
    - encapsulation on interfaces, disabling before
      - modifying.....1293
    - files See packet capture files
    - firewall filters, configuring.....1287
    - firewall filters, overview.....1247
    - IDP.....1998
    - J-Web tool.....1503
    - overview.....1246
    - overview (J-Web).....1503
    - preparation.....1282
    - verifying captured packets.....1284
    - verifying configuration.....1284
    - verifying firewall filter for.....1289
  - packet capture configuration
    - datapath debugging.....1289, 2179

packet capture files		
analyzing.....	1248	
libpcap format.....	1284	
overview.....	1247	
renaming before modifying encapsulation on		
interfaces.....	1293	
Packet Capture page		
field summary.....	1504	
results.....	1507	
packet encapsulation		
troubleshooting on the link services		
interface.....	1618	
verifying on the link services interface.....	1621	
packet filtering		
supported software standards.....	2297	
Packet Forwarding Engine		
MIB.....	1737, 1743, 1748, 1754	
packet fragmentation		
troubleshooting on the link services		
interface.....	1618	
verifying on the link services interface.....	1620	
packet headers, transmitted, displaying.....	1516	
packet loss priority, CoS.....	1373	
packet-capture statement.....	1340	
packet-filter statement		
security.....	1341	
packet-log statement.....	2104	
(Security IDP Sensor Configuration).....	2105	
packets		
capturing.....	1246	
capturing with J-Web packet capture.....	1503	
monitoring jitter.....	1507	
monitoring packet loss.....	1507	
monitoring round-trip times.....	1507	
multicast, tracking .....	1356	
packet capture.....	1246	
packet capture (J-Web).....	1503	
tracking MPLS.....	1494	
tracking with J-Web traceroute.....	1483	
pages, layout in J-Web.....	580	
parameters statement.....	1922	
usage guidelines.....	1849	
parentheses, in syntax descriptions.....	lx	
partial command entry, completing.....	518	
partition, storage medium.....	625	
password.....	18, 26	
password retry limits, setting.....	923	
passwords		
for downloading software upgrades.....	174	
local password method for user		
authentication.....	900	
<i>See also</i> local password		
retry limits.....	923	
root password, recovering.....	1612	
setting login retry limits.....	923	
srx root password, recovering.....	1614	
paste command		
usage guidelines.....	337	
pattern statement		
(Security IDP).....	2105	
PC <i>See</i> management device		
PCAP <i>See</i> packet capture		
peer entities.....	445	
peer statement.....	815	
peers, BGP <i>See</i> BGP neighbors; BGP RPM probes		
performance indicators.....	1808	
performance statement.....	2106	
performance, monitoring <i>See</i> RPM		
permission bits, for login classes.....	674	
permission flags		
login class.....	1059	
user.....	1059	
permissions		
denying and allowing commands.....	675	
predefined.....	673	
permissions statement		
usage guidelines.....	1059	
permissions, CLI, displaying.....	530, 1227	
pfe (system logging facility).....	1642	
PGM		
supported software standards.....	2301	
physical interfaces, CoS.....	1367	
PIM		
supported software standards.....	2301	
PIMs (Physical Interface Modules)		
checking power and heat status.....	1448	
ping		
ATM.....	656	
host.....	653	
host reachability (CLI).....	1486	
host reachability (J-Web).....	1488	
ICMP probes.....	1294	
MPLS.....	655	
RPM probes <i>See</i> RPM probes		
TCP and UDP probes.....	1298	

- ping command.....1486
  - DHCP server operation.....713
  - DHCP server operation, explanation.....713
  - options.....1486
- Ping end point of LSP
  - description.....1244
  - using.....1491
- ping host
  - results.....658
  - sample.....657
- Ping Host page
  - field summary.....1488
- Ping LDP-signaled LSP
  - description.....1244
  - using.....1491
- 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.....1244
  - using.....1491
- Ping MIB.....1738, 1743, 1748, 1754
  - use in ping test.....1966
  - view configuration example
    - SNMP.....1822
- 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.....604
  - RSVP-signaled LSP.....655
- ping MPLS (J-Web)
  - indications.....1494
  - Layer 2 circuits.....1244
  - Layer 2 VPNs.....1244
  - Layer 3 VPNs.....1244
  - LSP state.....1244
  - options.....1244
  - requirements.....1281
  - results.....1494
- ping mpls l2circuit command.....1494, 1531
  - results.....1494
- ping mpls l2vpn command.....1495, 1528
  - results.....1494
- ping mpls l3vpn command.....1497, 1534
  - results.....1494
- ping mpls ldp command.....1498, 1536
  - results.....1494
- ping mpls lsp-end-point command.....1498, 1539
  - results.....1494
- Ping MPLS page
  - field summary.....1491
  - results.....1494
- ping mpls rsvp command.....1498, 1541
  - results.....1494
- Ping RSVP-signaled LSP
  - description.....1244
  - using.....1491
- pingProbeHistoryTable.....1976
- pipe ( | )
  - command output, filtering.....328, 533
- pipe (I) command, to filter output.....1231
- Point-to-Point Protocol See PPP
- Point-to-Point Protocol over Ethernet See PPPoE
- policers, displaying.....109
- Policy Objects MIB.....1738, 1743, 1748, 1754
- policy options, configuration summary.....596
- policy-lookup-cache statement.....2106
- port settings.....3
- port statement.....1684
  - SNMPv3.....1922
  - usage guidelines.....1848
- ports
  - alarm conditions and configuration
    - options.....1238
  - configuring alarms on.....1276
  - console port, securing.....681
  - DHCP interface restrictions.....689
  - individual port types.....1238
  - monitoring.....1382
- post-attack statement.....2107
- post-attack-timeout statement.....2107
- power management, chassis.....1448
- PPP (Point-to-Point Protocol)
  - monitoring (CLI).....1403
- PPP encapsulation
  - on the link services interface.....1621
- PPP interfaces
  - supported software standards.....2286
- PPP MIB.....1721
- PPPoE (Point-to-Point Protocol over Ethernet)
  - interfaces.....1404
  - monitoring.....1404
  - session status.....1404

statistics.....	1404	profiles, accounting	
version information.....	1404	filter.....	1263
PPPoE, monitoring.....	632	interface.....	1260
pre-attack statement.....	2108	MIB.....	1272
pre-filter-shellcode statement.....	2108	Routing Engine.....	1274
predefined profiles.....	10	programs	
predefined-attack-groups statement.....	2109	managing.....	503
predefined-attacks statement.....	2109	prompt	
prefix list		setting to display in CLI.....	521
adding to SNMP community.....	1863	to restart.....	522
prefix statement.....	817	prompt strings	
priorities		CLI.....	510
system logging, including in log message		protect command.....	475
for single-chassis system.....	1662	usage guidelines.....	399
privacy-3des statement.....	1923	protecting configuration	
usage guidelines.....	1832	usage guidelines.....	399
privacy-aes128 statement.....	1924	protocol statement	
usage guidelines.....	1831	(Security IDP IP Headers).....	2114
privacy-des statement.....	1925	(Security IDP Signature Attack).....	2115
usage guidelines.....	1832	protocol-binding statement.....	2112
privacy-none statement.....	1925	protocol-name statement.....	2113
usage guidelines.....	1832	protocols	
privacy-password statement.....	1926	DHCP See DHCP	
usage guidelines		originating, displaying.....	1415
for 3DES algorithm.....	1832	OSPF, monitoring.....	1417
for AES algorithm.....	1831	PPP, monitoring.....	1403
for DES algorithm.....	1832	RIP, monitoring.....	1416
probe loss		routing protocols, monitoring.....	1413, 1419
monitoring.....	1507	PVCs (permanent virtual circuits)	
threshold, setting.....	1306	preventing dropped packets on.....	1625
probe statement			
RPM.....	1342	<b>Q</b>	
probe-interval statement.....	1343	Quick Configuration	
probe-limit statement.....	1343	basic settings.....	588
probe-server statement.....	1344	initial configuration.....	588
probe-type statement.....	1345	RPM pages.....	1294
probes, monitoring.....	1404, 1507	quit command.....	320, 476, 513
See also RPM probes		usage guidelines.....	337
Process Details		<b>R</b>	
monitoring.....	637	RADIUS	
process-ignore-s2c statement.....	2110	authentication (configuration editor).....	895
process-override statement.....	2110	order of user authentication (configuration	
process-port statement.....	2111	editor).....	900
processes		secret (configuration editor).....	895
managing.....	503	specifying for authentication .....	900
restarting.....	547, 1006	supported software standards.....	2282
products statement.....	2111	random early detection (RED) drop profiles,	
		CoS.....	1370

- 
- rapid commit.....740
  - rapid-commit statement.....819
  - RARP, for autoinstallation.....205
  - re-assembler statement.....2118
  - re-generate-keypair.....1670
  - reO configuration group.....428
  - re1 configuration group.....428
  - read-only login class permissions.....673
  - read-view statement.....1927
    - usage guidelines.....1856
  - real-time monitoring
    - files.....1512, 1703
    - traffic.....1516
  - real-time performance monitoring See RPM
  - reboot immediately .....627
  - recommended-action statement.....2119
  - reconfigure statement
    - DHCP local server.....820
  - recovery software installation.....136
  - red asterisk (\*).....582
  - RED drop profiles, CoS.....1370
  - redrawing screen.....348
  - Refresh button.....607
  - refresh-timeout statement.....2119
  - regaining DHCP lease after initial
    - configuration.....589
  - regex statement.....2120
  - regional configurations.....447
  - registration form, for software upgrades.....166
  - regular expression operators
    - system logging.....1665
  - regular expressions
    - first match, displaying from.....331
    - matching output, displaying.....332
    - nonmatching output, ignoring.....331
  - regular expressions for filtering events.....621
  - reject-timeout statement.....2120
  - relational operators, for multicast traffic.....1503
  - relative option.....423
  - release names.....132
  - remote accounts
    - accessing with SSH (CLI).....929
    - accessing with Telnet (CLI).....928
    - remote template accounts.....908
  - remote connection to router
    - connecting USB modem to router.....679
  - remote operations MIBs.....1803
  - remote server, upgrading from.....185
  - remote template accounts.....908
  - remote-engine statement.....1928
  - removing
    - files.....970
  - rename command.....477, 478
    - usage guidelines.....385
  - renaming files.....972
  - renaming identifiers.....385
  - replace command.....479
    - usage guidelines.....349
  - replace option.....422
  - req-option statement.....821
  - request command.....545
    - usage guidelines.....320, 512
  - request interface modem reset umd0
    - command.....922
  - request message filter.....333
  - request pppoe connect command.....1546
  - request pppoe disconnect command.....1547
  - request security datapath-debug capture start
    - command.....2199
  - request security idp security-package download
    - command.....2200
  - request security idp security-package install
    - command.....2202
  - request security idp ssl-inspection key add
    - command.....2204
  - request security idp ssl-inspection key delete
    - command.....2206
  - request security idp storage-cleanup
    - command.....2208
  - request support information command.....995
  - request system autorecovery state
    - command.....273, 976
  - request system configuration rescue delete
    - command.....573, 575
  - request system configuration rescue save
    - command.....573, 575
  - request system download abort
    - command.....275, 978
  - request system download clear
    - command.....276, 979
  - request system download pause
    - command.....277, 980
  - request system download resume
    - command.....278, 981
  - request system download start
    - command.....279, 982
  - request system firmware upgrade
    - command.....280, 983

request system halt command.....	507	restart routing command.....	506
request system license add command.....	257, 941	restarting	
request system license add terminal		after software upgrade.....	511, 522
command.....	257, 941	software processes.....	547, 1006
request system license delete		retransmission-attempt statement.....	822
command.....	260, 945	retransmission-interval (dhcp-client)	
request system license save command.....	255, 940	statement.....	823
request system license update		retry limits for passwords.....	923
command.....	98, 256, 281, 941, 984	retry-count statement.....	1929
request system logout pid pid_number		usage guidelines.....	1867
command.....	367	Reverse Address Resolution Protocol (RARP), for	
request system partition compact-flash		autoinstallation.....	205
command.....	282, 985	reverse SSH.....	683
request system power-off fpc		reverse ssh port.....	816
command.....	283, 986	reverse Telnet.....	683
request system reboot.....	289, 993	reverse telnet.....	832
request system reboot command.....	507	reverse telnet port.....	816
request system services dhcp command.....	987	Reverse-Path-Forwarding	
request system set-encryption-key algorithm des		MIB.....	1738, 1743, 1749, 1754
command.....	932	reverse-ssh.....	823
request system set-encryption-key		reverting to a previous configuration file	
command.....	932	(J-Web).....	199
request system set-encryption-key des		rewrite rules, CoS.....	1372
unique.....	932	RFCs supported See Index of Supported Software	
request system set-encryption-key unique.....	932	Standards	
request system snapshot.....	136, 284, 988	RIP	
request system software abort in-service-upgrade		supported software standards.....	2309
command.....	287, 991	RIP (Routing Information Protocol)	
request system software add .....	288, 992	monitoring.....	1416
request system software rollback.....	136, 290, 994	statistics.....	1416
request system storage cleanup command.....	935	RIP neighbors	
request system storage cleanup dry-run		displaying.....	1416
command.....	935	status.....	1416
request-type statement.....	1929	RIP routing information.....	1416
RMON		RIPng	
usage guidelines.....	1873	supported software standards.....	2309
required entry .....	582	rising-event-index statement.....	1930
rescue configuration		usage guidelines.....	1871
deleting .....	648	rising-threshold statement	
setting .....	648	health monitor.....	1931
viewing .....	648	RMON.....	1930
rescue configuration, alarm about.....	1241	RJ-45 to DB-9 serial port adapter.....	1612
reset statement		RMON alarm entries.....	1870
(Security IDP).....	2121	RMON alarms.....	1804, 1811
reset-on-policy statement.....	2121	RMON event entries.....	1874
resolve command.....	533	RMON events.....	1806, 1810
Resource Reservation Protocol See RSVP		RMON Events and Alarms	
restart command.....	547, 1006	MIB.....	1738, 1743, 1749, 1755
usage guidelines.....	320, 512		

- 
- rmon statement.....1931
    - usage guidelines.....1810
  - roles
    - example.....914
  - rollback command.....480, 575
    - usage guidelines.....337
  - rolling back a configuration file during
    - configuration.....645
  - rolling back a configuration file, to downgrade
    - software (CLI).....199
  - rollover cable, connecting the console port.....1612
  - root login to the console, disabling.....681
  - root password recovery.....1612, 1614
  - root password, defining (Quick Configuration).....589
  - rotating files.....934
  - round-trip time
    - description.....1250
      - See also* RPM probes
    - threshold, setting.....1306
  - route information sample task.....640
  - router.conf file, for autoinstallation.....153
  - routers
    - login classes.....1063
    - storage media.....135
  - routes, displaying
    - to specified network host.....1608
  - routing
    - monitoring.....633, 1413
    - traceroute (J-Web).....1483
  - Routing Engine profile.....1274
  - Routing Engines
    - storage media
      - J Series routers.....135
    - synchronizing configuration.....426
  - routing instances
    - access lists
      - configuring.....1861
    - SNMP
      - enabling access.....1858
      - identifying.....1797
      - specifying.....1858
  - routing instances, configuration summary.....596
  - routing options, configuration summary.....597
  - routing protocols
    - configuration summary.....596
  - routing solutions
    - applying CoS components on link services
      - interface.....1617
    - load balancing on link services
      - interfaces.....1618
    - preventing dropped packets on PVCs.....1625
    - reducing jitter and latency on multilink
      - bundles.....1618
  - routing table
    - monitoring.....1414
  - routing, monitoring.....633, 1413
  - routing-engine-profile statement.....1346
    - usage guidelines.....1274
  - routing-instance statement
    - SNMP.....1934
    - SNMPv3.....1935
      - usage guidelines.....1848
  - routing-instance-access.....1935
  - RPC
    - displaying command output in.....331
  - rpc statement.....2122
  - RPM
    - supported software standards.....2312
  - RPM (real-time performance monitoring)
    - basic probes (configuration editor).....1294
    - BGP monitoring *See* BGP RPM probes
    - graph results.....633
    - inbound and outbound times.....1250
    - jitter, viewing.....1507
    - monitoring.....632
    - monitoring probes.....1507
    - overview.....1249
      - See also* RPM probes
    - preparation.....1294
    - probe and test intervals.....1250
    - probe counts.....1250
    - Quick Configuration.....1294
    - round-trip times, description.....1250
    - round-trip times, viewing.....1507
    - RPM probes.....633
    - sample configuration.....1297
    - sample graphs.....633, 1507
    - statistics.....1250
    - statistics, verifying.....1297
    - TCP probes (configuration editor).....1298
      - See also* TCP RPM probes
    - tests.....1249
    - tests, viewing.....1507
    - threshold values.....1252



tuning probes.....	1305	timestamps See RPM probe timestamps	
UDP probes (configuration editor).....	1298	tuning.....	1305
See also UDP RPM probes		UDP (configuration editor).....	1298
verifying probe servers.....	1300	See also UDP RPM probes	
RPM pages.....	1294	UDP server port.....	1306
field summary.....	1306	verifying TCP and UDP probe servers.....	1300
RPM probe timestamps		RSVP	
overview.....	1250	LSP connections	
setting (configuration editor).....	1294	operability, checking.....	1541
RPM probes		supported software standards.....	2295
basic (configuration editor).....	1294	RSVP (Resource Reservation Protocol)	
BGP neighbors See BGP RPM probes		interfaces, monitoring.....	1391
cumulative jitter.....	1507	sessions, monitoring.....	1389
current tests.....	1507	RSVP LSPs	
DSCP bits (Quick Configuration).....	1306	ping interval.....	1541
graph results.....	1507	RTT See RPM probes, round-trip times	
ICMP (configuration editor).....	1294	rule statement	
inbound times.....	1250	(Security DDoS Rulebase).....	2124
jitter threshold.....	1306	(Security Exempt Rulebase).....	2123
monitoring.....	1507	(Security IPS Rulebase).....	2125
outbound times.....	1250	rulebase-ddos statement.....	2127
probe count, setting (Quick		rulebase-exempt statement.....	2128
Configuration).....	1306	rulebase-ips statement.....	2129
probe count, tuning.....	1305	run command.....	481
probe counts.....	1250	usage guidelines.....	337
probe intervals.....	1250		
probe intervals, setting (Quick		<b>S</b>	
Configuration).....	1306	sample configuration	
probe intervals, tuning.....	1305	for secure access.....	893
probe loss count.....	1306	for SSL certificates.....	893
probe owner.....	1306	sample tasks	
probe type, setting (Quick		configuring accounting options.....	608
Configuration).....	1306	filtering and viewing events.....	622
probe types.....	1249	managing snapshots.....	626
round-trip time threshold.....	1306	monitoring interfaces.....	638
round-trip times, description.....	1250	monitoring route information.....	640
round-trip times, viewing.....	1507	ping host.....	657
SNMP traps (Quick Configuration).....	1306	viewing alarms.....	616
source address, setting.....	1305	sample-type statement.....	1936
TCP (configuration editor).....	1298	usage guidelines	
See also TCP RPM probes		for alarms.....	1873
TCP server port.....	1306	for events.....	1874
test intervals.....	1250	samples	
test intervals, setting (Quick		alarm configuration.....	1278
Configuration).....	1306	basic RPM probes.....	1294
test target.....	1306	local template account.....	908
threshold values, description.....	1252	RPM probes.....	1297
threshold values, setting (Quick		RPM test graphs.....	1507
Configuration).....	1306		



- TCP and UDP probes.....1298
- user account.....902
- SAP
  - supported software standards.....2301
- save command.....482, 533
  - usage guidelines.....337, 573
- saving licenses (CLI).....255, 940
- scheduler maps, CoS.....1373
- scheduling a reboot.....627
- scope statement
  - (Security IDP Chain Attack).....2130
  - (Security IDP Custom Attack).....2131
- screen
  - dimensions.....509, 514
  - redrawing.....348
- screen length, setting.....523
- screen width, setting.....524
- SDH
  - supported software standards.....2287
- SDP
  - supported software standards.....2301
- secret
  - RADIUS (configuration editor).....895
  - TACACS+ (configuration editor).....897
- secure access
  - establishing.....663
  - generating SSL certificates.....592, 888
  - HTTPS access.....612, 890
  - HTTPS access (configuration editor).....892
  - HTTPS recommended.....591, 663
  - installing SSL certificates.....612, 890
  - installing SSL certificates (configuration editor).....892
  - Junos XML protocol SSL access.....890
  - JUNOScript SSL access.....612
  - overview.....663
  - requirements.....888
  - sample configuration.....893
  - verifying secure access configuration.....893
- Secure Access page
  - description.....612
  - field summary.....613
- Secure Sockets Layer See SSL
- security
  - access privileges.....673, 902
  - alarms.....1592
  - console port security.....681
  - log.....1700
  - log file.....1702
  - NAT.....9
  - packet capture for intrusion detection.....1246
  - password retry limits.....923
  - policies.....8
    - configuration.....39
  - user accounts.....672, 902
  - user authentication.....671
  - zones.....8
    - configuration.....39
- Security Configuration Statement
  - Hierarchy.....58, 2005
- Security Interface Extension Objects
  - MIB.....1738, 1743, 1749, 1755
- security log file
  - binary format.....1645
- security logs.....1654
  - streaming through revenue ports.....1654
- security policy
  - DNS name resolution.....1616
- Security Screening Objects MIB.....1738, 1749, 1755
- security, configuration summary.....597
- security-level statement
  - for access privileges.....1937
    - usage guidelines.....1855
  - for SNMP notifications.....1938
    - usage guidelines.....1851
- security-log-percent-full
  - security alarms.....1685
- security-model statement
  - for access privileges.....1939
    - usage guidelines.....1854
  - for groups.....1940
    - usage guidelines.....1833
  - for SNMP notifications.....1940
    - usage guidelines.....1851
- security-name statement
  - for community string.....1941
  - for security group.....1941
    - usage guidelines.....1833
  - for SNMP notifications.....1942
    - usage guidelines.....1851
- security-package statement.....2132
- security-to-group statement.....1943
  - usage guidelines.....1853
- sensor-configuration statement.....2133
- sequence-number statement
  - (Security IDP ICMP Headers).....2135
  - (Security IDP TCP Headers).....2136
- serial cable, disconnection for console logout.....681

serial interfaces		set cli directory command.....	519
supported software standards.....	2288	usage guidelines.....	510
Serial Line Address Resolution Protocol (SLARP),		set cli idle-timeout command.....	520
for autoinstallation.....	205	usage guidelines.....	511
serial ports		set cli prompt command.....	521
alarm conditions and configuration		usage guidelines.....	510
options.....	1238	set cli restart-on-upgrade command.....	522
autoinstallation on.....	152	usage guidelines.....	511
configuring alarms on.....	1276	set cli screen-length command.....	523
Series		usage guidelines.....	509, 514
user interfaces See user interfaces		set cli screen-width command.....	524
server address statement.....	826	set cli terminal command.....	525
server statement		usage guidelines.....	510
NTP.....	825	set cli timestamp command.....	526
service quality		usage guidelines.....	510
monitoring.....	1807	set command.....	341
service sets, monitoring.....	636	configuration mode.....	484, 557
service statement		usage guidelines.....	337
(Security Dynamic Attack Group).....	2137	set date command.....	527
(Security IDP Anomaly Attack).....	2136	set no-encrypt-configuration-files command.....	932
services gateway		set option.....	423
autoinstallation.....	156	Set requests, SNMP.....	1716
Services Gateway		Set Up page	
licenses.....	157, 696	field summary.....	589
user interfaces See user interfaces		prerequisites.....	588
services module		setup	
alarm conditions and configuration		Quick Configuration.....	588
options.....	1238	requirements.....	588
Services Router		severity	
as a DHCP server.....	684	security log.....	1686
licenses.....	157, 696	severity levels	
monitoring .....	1231	for alarms See alarm severity	
performance monitoring.....	1249	severity levels for events.....	619
user interfaces See user interfaces		severity statement	
services statement		(Security Dynamic Attack Group).....	2139
remote router access.....	827	(Security IDP Custom Attack).....	2138
services, configuration summary.....	597	(Security IDP IPS Rulebase).....	2140
sessions		SHA-1 (Secure Hash Algorithm) checksum.....	137
BGP peer, status details.....	1419	sha-256 checksum, calculating.....	964
limiting number of.....	611	SHA-1 checksum, calculating.....	963
limits.....	611	shellcode statement.....	2141
RSVP, monitoring.....	1389	show bgp neighbor command.....	1419
Telnet.....	928	show bgp summary command.....	1419
terminating.....	612	show chassis alarms command.....	1278, 1477, 1551
sessions statement.....	2137	show chassis environment command.....	1448
sessions, J-Web.....	671	show chassis hardware	
set cli complete-on-space command.....	518	command.....	1445, 1447, 1448
usage guidelines.....	511	show chassis power-ratings command.....	1448

- 
- show chassis redundant-power-supply
    - command.....1448
  - show chassis routing-engine.....134
  - show chassis routing-engine bios.....198
  - show chassis routing-engine
    - command.....1012, 1448, 1450
  - show chassis usb storage command.....291
  - show class-of-service classifier
    - command.....1368, 1375
  - show class-of-service code-point-aliases
    - command.....1369
  - show class-of-service drop-profile
    - command.....1370
  - show class-of-service forwarding-class
    - command.....1371
  - show class-of-service rewrite-rules
    - command.....1372
  - show class-of-service scheduler-map
    - command.....1373
  - show cli authorization command.....530, 1227
  - show cli command.....528
    - usage guidelines.....511
  - show cli directory command.....531
  - show cli history command.....532
    - usage guidelines.....455
  - show command
    - configuration mode.....558
    - usage guidelines.....337
  - show configuration command.....559, 1548
  - show dhcpv6 server binding.....1031
  - show dhcpv6 server statistics command.....1035
  - show firewall command.....1038
  - show firewall filter dest-all command.....1289
  - show groups junos-defaults command.....566
    - usage guidelines.....450
  - show interfaces command.....1553
  - show interfaces detail command.....1382
  - show interfaces dl0 extensive command.....704
  - show interfaces interface-name command.....1382
  - show interfaces pp0 command.....1404
  - show interfaces terse command.....1382
  - show log command.....1643, 1707
  - show mpls interface command.....1387
  - show mpls lsp command.....1387
  - show mpls statistics command.....1388
  - show ospf interfaces command.....1417
  - show ospf neighbors command.....1417
  - show ospf statistics command.....1417
  - show poe interface command.....1582
  - show poe telemetries interface.....1584
  - show ppp address-pool command.....1403
  - show ppp interface command.....1403
  - show ppp statistics command.....1403
  - show ppp summary command.....1403
  - show pppoe interfaces command.....1404, 1586
  - show pppoe statistics command.....1404, 1590
  - show pppoe version command.....1404
  - show redundant-power-supply command.....1448
  - show rip neighbors command.....1416
  - show rip statistics command.....1416
  - show route detail command.....1414
  - show route terse command.....1414
  - show security alarms command.....1592
  - show security datapath-debug capture.....1596
  - show security datapath-debug counter.....1597
  - show security flow session command.....102
  - show security flow session idp family
    - command.....2210
  - show security idp active-policy
    - command.....99, 2214
  - show security idp application-ddos
    - command.....2215
  - show security idp attack description
    - command.....2217
  - show security idp attack detail command.....2218
  - show security idp attack table command.....2220
  - show security idp counters application-ddos
    - command.....2221
  - show security idp counters
    - application-identification command.....2224
  - show security idp counters dfa command.....2226
  - show security idp counters flow command.....2227
  - show security idp counters ips command.....2235
  - show security idp counters log command.....2238
  - show security idp counters packet command.....2241
  - show security idp counters packet-log
    - command.....2244
  - show security idp counters policy-manager
    - command.....2246
  - show security idp counters tcp-reassembler
    - command.....2247
  - show security idp logical-system policy-association
    - command.....2250
  - show security idp memory command.....2251
  - show security idp policies.....2252
  - show security idp policy-commit-status clear
    - command.....2254

show security idp policy-commit-status		
command.....	2253	
show security idp policy-templates.....	2255	
show security idp predefined-attacks.....	2256	
show security idp security-package-version		
command.....	2258	
show security idp ssl-inspection key		
command.....	2259	
show security idp ssl-inspection session-id-cache		
command.....	2261	
show security idp status command.....	100, 2262	
show security idp status detail.....	2264	
show security log command.....	1709	
show security log file command.....	1712	
show security monitoring fpc fpc-number		
command.....	1598	
show security nat destination summary		
command.....	107	
show security policies command.....	109	
show security utm session.....	116	
show security utm status.....	117	
show security zones command.....	118	
show services rpm active-servers		
command.....	1300, 1303	
explanation.....	1300, 1303	
show services rpm probe-results		
command.....	1297, 1507, 1603	
explanation.....	1297	
show snmp mib command.....	1991	
show system alarms command.....	1607	
show system auto-snapshot command.....	294	
show system autoinstallation status		
command.....	207	
show system autorecovery state		
command.....	292, 1040	
show system commit command.....	567	
show system download command.....	296, 1044	
show system license		
command.....	121, 259, 261, 298, 944, 946, 1046	
explanation.....	259, 261, 944, 946	
show system license keys command.....	259, 944	
show system license usage command.....	259, 944	
explanation.....	259, 944	
show system login lockout command.....	301, 1049	
show system process command.....	1450	
show system processes command.....	1643	
show system processes extensive command.....	504	
output, table.....	505	
show system services dhcp binding command.....	712	
show system services dhcp binding detail		
command.....	712	
show system services dhcp client		
command.....	124, 717, 1050	
show system services dhcp client interface		
command.....	717	
show system services dhcp client statistics		
command.....	718	
show system services dhcp conflict		
command.....	688	
show system services dhcp global command.....	712	
show system services dhcp relay-statistics		
command.....	722, 1053	
explanation.....	722	
show system snapshot media.....	212, 214, 302, 1055	
show system statistics command.....	567	
show system storage.....	134	
show system storage command.....	1445, 1447	
show system storage		
partitions.....	303, 305, 1056, 1058	
show system uptime command.....	1445, 1447	
show system users command.....	1445, 1447	
show version.....	170	
show version command.....	170, 1445, 1447	
Junos OS.....	502	
show   display inheritance command.....	562	
show   display inheritance defaults command		
usage guidelines.....	450	
show   display omit command.....	563	
show   display set command.....	564	
usage guidelines.....	361	
show   display set relative.....	565	
show   display set relative command.....	565	
usage guidelines.....	362	
show forwarding-options command.....	1284	
side pane, J-Web.....	582	
signature statement		
(Security IDP).....	2142	
SIP		
supported software standard.....	2312	
SIP timeouts		
media inactivity.....	1999	
size statement.....	1687	
accounting.....	1349	
usage guidelines.....	1259	
archiving of all system log files.....	1669	
SLARP, for autoinstallation.....	205	

- snapshot
  - sample task.....626
  - system software.....625
- SNMP
  - adding client lists and prefix lists.....1863
  - agent.....1716, 1718
  - architecture.....1716
  - commit delay timer.....1817
  - community string.....1862
  - configuration
    - version 3.....1885
    - versions 1 and 2.....1813
  - configuration summary.....597
  - filtering duplicate requests.....1819
  - limiting interface access.....1820
  - logging, enabling.....1804
  - manager.....1716
  - master agent.....1718
  - MIB object values, displaying.....1991
  - MIB views.....1821
  - remote operations.....1801
  - standard traps See SNMP traps
  - standards documents.....1719
  - subagent.....1718
  - system contact.....1815
  - system description.....1815
  - system location.....1816, 1915
  - system name.....1816
  - tracing operations.....1968
  - trap groups.....1841
  - trap notification for remote operations.....1803
  - trap options.....1837
  - views, setting.....1802
- SNMP informs.....1823
- snmp statement.....1943
  - usage guidelines
    - SNMPv1 and SNMPv2.....1813
    - SNMPv3.....1885
- SNMP traps.....1717
  - performance monitoring See RPM probes
  - source address configuration.....1837
  - standard
    - version 1.....1786
    - version 2.....1789
  - system logging severity levels.....1718
  - unsupported.....1793
- snmp-community statement.....1944
- SNMPv2
  - MPLS traps.....1792
  - Passive Monitoring Traps MIB.....1841
- SNMPv3
  - authentication, configuring.....1830
  - informs, configuring.....1823
  - local engine ID, configuring.....1823
  - minimum configuration.....1828
- software installation
  - category change installation
    - description.....136
  - recovery installation
    - description.....136
  - standard installation
    - description.....136
- software installation packages.....131
  - standard Junos OS for J Series routers,
    - domestic
      - description.....131
- software package
  - downgrading.....623
  - installing.....623
  - upgrading.....623
- software packages
  - upgrading individual.....164
- software upgrade
  - restarting after.....522
- software, halting immediately.....627
- SONET
  - supported software standards.....2287
- Source Class Usage MIB.....1739, 1749, 1755
- source statement
  - (Security IDP IP Headers).....2146
- source-address statement.....1944
  - (Security IDP Policy).....2147
  - (Security IDP Sensor Configuration).....2147
  - NTP.....832
  - RADIUS and TACACS+.....832
  - system logging.....832
  - usage guidelines.....1837
- source-classes statement.....1349
  - usage guidelines.....1270
- source-except statement.....2148
- source-port statement
  - (Security IDP).....2148
- SPU Monitoring MIB.....1739, 1749
- SPU monitoring MIB.....1755
- SRC application.....664

SRX Series.....	695	SSH	
alarms.....	1237	accessing remote accounts (CLI).....	929
licenses.....	157, 696	setting login retry limits.....	923
managing user authentication.....	671	ssh command.....	929
monitoring .....	1231	options.....	929
packet capture.....	1246	usage guidelines.....	320, 512
performance monitoring.....	1249	SSH, defining access (Quick Configuration).....	591
system log messages.....	1643	ssh-known-hosts statement.....	824
SRX Series devices		SSL (Secure Sockets Layer)	
software upgrades.....	137	enabling secure access.....	612, 890
SRX Series Services Gateway.....	210 See storage	management access.....	663
m          e          d          i          a		verifying SSL configuration.....	893
auto bios upgrade methods.....	149	SSL 3.0 option, disabling on Internet Explorer for	
boot devices		worldwide version of Junos OS.....	587, 666
configuring (CLI).....	210	SSL access, establishing.....	663
configuring (J-Web).....	210	SSL certificates	
Chassis Components		adding.....	894
Offline.....	270	adding (configuration editor).....	892
Online.....	270	adding (Quick Configuration).....	613
configuring boot devices.....	210	generating.....	592, 888
dual-root partitioning.....	145	sample configuration.....	893
halting a with J-Web.....	266	verifying SSL configuration.....	893
halting immediately (CLI) .....	266	ssl-inspection statement.....	2149
halting with the CLI.....	266	standard software installation.....	136
Install Remote page		standard traps, SNMP	
field summary.....	210	version 1.....	1786
installing earlier version of Junos OS		version 2.....	1789
with dual-root.....	191	standards documents	
installing software		SNMP and MIBs.....	1720
with CLI.....	193	start-log statement.....	2149
with J-Web.....	193	start-time statement	
Junos OS Release 10.0		(Security IDP).....	2150
upgrading with dual-root.....	192	accounting.....	1350
upgrading without dual-root.....	138	usage guidelines.....	1259
multiple devices, using snapshots to replicate		startup	
configurations		J-Web interface.....	586, 666
J-Web.....	210	startup, J-Web interface.....	586, 666
rebooting (CLI).....	262	startup-alarm statement.....	1945
rebooting with J-Web .....	262	usage guidelines.....	1873
reboots.....	262, 266	stateful firewall.....	7
recover of primary image.....	190	statistics	
request system halt command.....	266	BGP.....	1419
request system reboot command.....	262	interfaces.....	1358
request system snapshot command.....	210	LSP.....	1389
show system storage partitions.....	196	OSPF.....	1417
Snapshot page.....	210	performance monitoring.....	1250
snapshots.....	210	PPPoE.....	1404
software upgrade methods.....	138	RIP.....	1416
See also boot devices		RPM, description.....	1250

- RPM, monitoring.....1507
- RPM, verifying.....1297
- statistics statement
  - (Security IDP).....2150
- status
  - autoinstallation.....207
  - BGP.....1419
  - license key.....158, 697
  - OSPF interfaces.....1417
  - OSPF neighbors.....1417
  - RIP neighbors.....1416
- status command.....485
  - usage guidelines.....337, 364
- storage media.....135
  - device names
    - J Series routers.....135
    - J Series routers.....135
- storing previous configurations.....354
- streaming security logs through revenue
  - ports.....1654
- strings
  - help about.....316
- Structure of Management Information
  - MIB.....1739, 1740, 1745
    - Junos OS for J Series and SRX Series devices,
      - for.....1740, 1745, 1751
- structured-data statement.....1688
  - usage guidelines.....1659
- subagent, SNMP.....1718
- super-user login class permissions.....673
- superuser login class permissions.....673
- support, technical See technical support
  - system information, displaying.....995
- suppression statement.....2151
- symbol.....333
- syntax conventions.....lix
- sysContact object, MIB II.....1815
- sysDescription object, MIB II.....1815
- sysLocation object, MIB II.....1816
- syslog See system logs
- syslog statement
  - system processes.....1689
- syslog-subtag statement.....1945
  - usage guidelines.....1874
- sysName object, MIB II.....1816
- system.....905
  - configuration summary.....597
  - login lockout.....301, 959, 1049
  - monitoring.....637
  - retry options.....905
- system access and access management
  - supported software standards.....2283
- System Configuration Statement
  - Hierarchy.....215, 839
- system contact, SNMP.....1815
- system description, SNMP.....1815
- system identification settings.....18, 26
- system location, SNMP.....1816, 1915
- system log messages
  - /var/log directory.....1652
  - capturing in a file (configuration editor).....1652
  - destinations.....1643, 1653
  - displaying at a terminal (configuration
    - editor).....621
  - event viewer.....1378, 1696
  - filtering.....619
  - monitoring (Quick Configuration).....1696
  - overview.....617, 1643
- System Log MIB.....1739, 1744, 1750, 1755
- system logging
  - disabling.....1666
  - examples.....1647
  - facilities
    - default for remote machine.....1660
    - for local machine.....1642
  - message descriptions
    - displaying.....1635
    - fields in.....1635
  - messages, displaying
    - generated by service on PIC.....1641
    - structured-data format.....1636
  - regular expression filtering.....1664
  - regular expression operators.....1665
  - timestamp, modifying.....1663
- system logging severity levels, SNMP traps.....1718
- system logs
  - control plane logs.....1644
  - data plane logs.....1644
  - enabling.....652
  - file cleanup .....649
  - file cleanup (CLI).....935
  - file cleanup (J-Web).....934
  - functions.....617, 1643
  - logging severity levels.....619
  - messages See system log messages See
    - system log messages
  - monitoring.....1481



overview.....	1643	target-address statement.....	1947
redundant syslog server.....	1643	usage guidelines.....	1846
remote system log server.....	1653	target-parameters statement.....	1948
sending through eventd.....	1653	usage guidelines.....	1849
system management		targets statement.....	1949
displaying log and trace file contents.....	1481	usage guidelines.....	1841
files.....	648	taskbar.....	581, 667
licenses.....	624	TCP	
login classes.....	673, 902	supported software standards.....	2302
reboots.....	627	TCP RPM probes	
software.....	623	CoS classification, destination interface	
system logs.....	1643	requirement.....	1298
template accounts.....	676, 908	CoS classification, use with caution.....	1298
user accounts.....	672, 902	description.....	1249
user authentication.....	671	server port.....	1306
system memory		setting.....	1298
J Series routers.....	134	verifying servers.....	1300
system name, SNMP.....	1816	tcp statement	
system services.....	6	(Security IDP Protocol Binding).....	2153
system statement.....	1687	(Security IDP Signature Attack).....	2154
system time		tcp-flags statement.....	2156
defining (Quick Configuration).....	590	technical support	
synchronizing (Quick Configuration).....	590	contacting JTAC.....	lx
		system information, displaying.....	995
<b>T</b>		telnet	
T1 ports		reverse.....	683
alarm conditions and configuration		reverse SSH.....	683
options.....	1238	Telnet	
configuring alarms on.....	1276	accessing remote accounts (CLI).....	928
T3 interfaces		setting login retry limits.....	923
supported software standards.....	2288	telnet command.....	928
T3 ports		options.....	928
alarm conditions and configuration		usage guidelines.....	320, 512
options.....	1238	Telnet session.....	928
configuring alarms on.....	1276	Telnet, defining access (Quick Configuration).....	591
TACACS+		template accounts	
authentication (configuration editor).....	897	description.....	676
order of user authentication (configuration		local accounts (configuration editor).....	908
editor).....	900	remote accounts (configuration editor).....	908
secret (configuration editor).....	897	temporary files	
specifying for authentication.....	900	cleaning up (CLI).....	935
supported software standards.....	2282	cleaning up (J-Web).....	934
tag statement.....	1946	downloading (J-Web).....	937
SNMPv3		for packet capture.....	1248
usage guidelines.....	1866	temporary files, cleaning up.....	649
usage guidelines.....	1845	terminal screen	
tag-list statement.....	1946	length, setting.....	523
usage guidelines.....	1848	width, setting.....	524
target statement.....	1350, 2152	terminal statement.....	2157



- terminal type.....510
  - setting.....525
- test statement
  - (Security IDP).....2157
- tests See RPM
- TFTP, for autoinstallation.....153
- then statement
  - (Security IDP Policy).....2158
  - (Security Rulebase DDos).....2159
- threshold values, for RPM probes See RPM probes
- thresholds statement
  - RPM.....1351
- time synchronization
  - supported software standards.....2283
- time to live See TTL
- time zone, defining (Quick Configuration).....590
- time-binding statement.....2160
- time-format statement.....1691
  - usage guidelines.....1663
- timeout sessions.....611
- timeout statement.....1949
  - (Security IDP Policy).....2160
  - usage guidelines.....1867
- timeout, user, setting.....520
- timestamp, CLI output, setting.....526
- timestamps
  - for RPM probes See RPM probe timestamps
  - suppressing in packet headers, in captured packets.....1504
  - suppressing in packet headers, in traffic monitoring.....1500
- to-zone statement
  - (Security IDP Policy).....2161
- top command.....486
  - usage guidelines.....337, 385
- top pane, J-Web.....580
- tos statement.....2162
- total-length statement.....2163
- total-memory statement.....2163
- trace files
  - display of
    - starting.....1513, 1704
    - stopping.....1515, 1706
  - monitoring.....1481
  - multicast, monitoring.....1482
  - status, displaying.....1512, 1703
- traceoptions
  - security log.....1692
- traceoptions statement.....487, 1950
  - (Security IDP).....2166
  - datapath-debug.....1352, 2164
  - DHCP local server.....833
  - SNMP
    - usage guidelines.....1968
- traceroute
  - CLI command.....1480
  - indications.....1484
  - J-Web tool.....1483
  - results.....1484
  - TTL increments.....1483
- traceroute command.....1480, 1608
  - options.....1480
- Traceroute MIB.....1739, 1744, 1750, 1756, 1869
- traceroute monitor
  - CLI command.....1360
- traceroute monitor command.....1360
  - options.....1360
  - results.....1361
- Traceroute page
  - field summary.....1483
- traceroute, overview.....656
- tracing.....1694
  - destination-override.....1694
- tracing operations
  - SNMP.....1968
- tracing routes
  - monitoring.....1526
- traffic
  - analyzing with packet capture.....1246
  - multicast, tracking.....1356
  - tracking with J-Web traceroute.....1483
- traffic, real-time monitoring.....1516
- transfer-interval statement
  - accounting.....1353
  - usage guidelines.....1259
- trap groups, SNMP.....1841
- trap notification for SNMP remote
  - operations.....1803
- trap-group statement.....1952
  - usage guidelines.....1841
- trap-options statement.....1953
  - usage guidelines.....1837
- traps
  - definition.....1717
  - SNMP version 1 traps
    - standard.....1786

SNMP version 2 traps	
standard.....	1789
unsupported.....	1793
traps statement.....	1354
trim command.....	533
Trivial File Transfer Protocol (TFTP), for	
autoinstallation.....	153
troubleshoot	
CLI terminal.....	601
network connectivity.....	653
packet capture.....	656
ping ATM.....	656
ping host.....	653
ping MPLS.....	655
traceroute.....	656
troubleshoot sample task.....	657
troubleshooting	
applying CoS components on link services	
interface.....	1617
Avaya VoIP.....	1627
DNS name resolution in security policy.....	1616
dropped packets on PVCs.....	1625
events.....	652
J-Web access.....	652
J-Web behavior.....	651
jitter and latency on multilink bundles.....	1618
LFI and load balancing on multilink	
bundles.....	1618
packet capture for analysis.....	1246
<i>See also</i> diagnosis; packet capture	
root password recovery.....	1612, 1614
router connectivity.....	651
trusted-key statement.....	835
TTL (time to live)	
default, in multicast path-tracking	
queries.....	1356
increments, in traceroute packets.....	1483
threshold, in multicast trace results.....	1357
total, in multicast trace results.....	1357
TTL (time to live), ping requests.....	659
ttl statement	
(Security IDP).....	2168
tunable-name statement.....	2169
tunable-value statement.....	2170
TX Matrix router	
configuration groups.....	428
configuration groups example.....	432
type checking, CLI.....	346

type statement.....	1954
(Security Dynamic Attack Group).....	2170
(Security IDP ICMP Headers).....	2171
usage guidelines.....	1845

## U

UDP	
supported software standards.....	2302
UDP RPM probes	
CoS classification, destination interface	
requirement.....	1298
CoS classification, use with caution.....	1298
description.....	1249
server port.....	1306
setting.....	1298
verifying servers.....	1300
udp statement	
(Security IDP Protocol Binding).....	2172
(Security IDP Signature Attack).....	2173
umd0.....	676
unauthorized login class permissions.....	673
unified threat management.....	10
UNIX operating system.....	309, 310
UNIX shell.....	311
unknown logging severity.....	619
unprotect command.....	488
usage guidelines.....	399
unprotecting configuration	
usage guidelines.....	399
unsupported standard SNMP traps.....	1793
up command.....	489
usage guidelines.....	337, 385
update command.....	490
usage guidelines.....	337, 368
update-router-advertisement statement.....	835
update-server (dhcp-client) statement.....	836
update-server statement.....	836
updating	
licenses (CLI).....	256, 941
updating configure private configuration.....	368
upgrade, restarting after.....	511
upgrades	
downloading.....	174
installing (CLI).....	177
installing by uploading.....	177
installing from remote server.....	185
requirements.....	166
upgrading Junos OS.....	623
upgrading or downgrading Junos OS.....	164

- 
- upgrading software.....511
    - prompt to restart after.....522
  - uploading a configuration file.....647
  - urgent-pointer statement.....2174
  - url statement
    - (Security IDP).....2174
  - URLs
    - software downloads.....174
  - URLs, specifying in commands.....500
  - usb.....251
  - USB modem connections
    - connecting dial-up modem at user end.....921
    - dialer interface *See* dialer interface, USB
    - modem
    - interface naming conventions.....676
    - requirements.....679
    - USB modem interface types.....676
    - verifying dialer interfaces.....704
  - USB modem interfaces
    - dialer interface *See* dialer interface, USB
    - modem
  - USB modems
    - AT commands.....678
    - default modem initialization commands.....678
    - initialization by device.....678
    - resetting.....922
  - use-interface statement.....837
  - user (system logging facility).....1642
  - user access
    - login classes.....1063
  - user accounts
    - authentication order (configuration editor).....900
    - configuration example.....372
    - contents.....672
    - creating (configuration editor).....902
    - for local users.....908
    - for remote users.....908
    - predefined login classes.....673
    - templates for.....676, 908
      - See also* template accounts
  - user interfaces
    - Junos Scope application.....664
    - overview.....664
    - preparation.....586, 666
    - SRC application.....664
  - user permission flags.....1059
  - user roles
    - example.....914
  - user statement
    - SNMPv3.....1954
    - system logging.....1695
      - usage guidelines.....1660
  - user timeout, setting.....520
  - user-id statement.....836
  - username
    - description.....672
    - specifying .....902
  - users
    - access privileges.....673, 902
    - accounts *See* user accounts
    - adding.....902
    - CLI permissions, displaying.....530, 1227
    - editing configuration
      - displaying.....364
      - multiple simultaneous users.....341, 351
    - login classes.....673, 902
    - logs, displaying.....1707
    - of CLI, monitoring.....497
    - predefined login classes.....673
    - template accounts *See* template accounts
    - usernames.....672
    - viewing.....612
  - using alarms tasks.....615
  - usm statement.....1955
  - Utility MIB.....1739, 1744, 1750, 1756
  - UTM.....10
    - antispam.....10
    - antivirus.....10
    - configuration.....50
    - profiles.....89
    - webfiltering.....10
  - utm-policy.....10
- ## V
- v3 statement.....1957
    - usage guidelines.....1885
  - vacm statement.....1959
    - usage guidelines.....1853
  - validating software compatibility.....175
  - var/log/mib2d file.....1968
  - var/log/snmpd file.....1968
  - variable statement.....1960
    - usage guidelines.....1874
  - variable-length string indexes.....1803
  - vendor-id statement.....837

verification	
active licenses.....	259, 261, 944, 946
alarm configurations.....	1278
autoinstallation.....	207
captured packets.....	1284
destination path (J-Web).....	1483
DHCP server operation.....	713
DHCP statistics.....	722
dialer interfaces.....	704
firewall filter for packet capture.....	1289
host reachability (CLI).....	1486
host reachability (J-Web).....	1488
license usage.....	259, 944
licenses .....	259, 261, 943, 946
load balancing on the link services	
interface.....	1622
LSPs (J-Web).....	1244
packet capture.....	1284
packet encapsulation on link services	
interface.....	1621
RPM configuration.....	1297
RPM probe servers.....	1300, 1303
RPM statistics.....	1297
secure access.....	893
tracing multicast paths.....	1356
version	
PPPoE, information about.....	1404
version statement	
SNMP.....	1960
usage guidelines.....	1841
version, license key.....	158, 697
view and edit	
committing a text file, with caution.....	599
configuration text, viewing.....	597
configuration, editing.....	595
uploading a file.....	647
View Configuration Text page.....	598
View Events page	
field summary (filtering log	
messages).....	620, 1414
overview.....	617
view statement	
SNMP (associating with community).....	1961
usage guidelines.....	1862
SNMP (configuring MIB view).....	1962
usage guidelines.....	1821
viewing alarms, sample task.....	616
viewing configuration text.....	597
viewing events, sample task.....	622
views, MIB	
SNMP.....	1802, 1821
VLAN.....	3
vlan.....	5
voice calls, not supported in dial-in .....	676
voice services	
supported software standards.....	2313
VoIP interface	
correcting version incompatibility	
problem.....	1627
unavailability, correcting.....	1627
VPLS	
supported software standards.....	2315
VPN	
IPsec.....	12
VPN Certificate Objects MIB.....	1739, 1744, 1750, 1756
VPN MIB.....	1740
vpn statement.....	838
VPNs	
carrier-of-carriers	
supported software standards.....	2313
interprovider	
supported software standards.....	2313
Layer 2	
supported software	
standards.....	2290, 2313
Layer 3	
supported software standards.....	2314
multicast	
supported software standards.....	2315
VPNs (virtual private networks), DHCP support on	
interfaces.....	689
<b>W</b>	
WAN.....	3
warning logging severity.....	619
Web access, secure See secure access	
Web browser, modifying Internet Explorer for	
worldwide version of Junos OS.....	587, 666
Web Filtering	
verifying.....	1476
web-management statement.....	885
wildcard characters.....	435
wildcard command.....	492
wildcard delete command	
usage guidelines.....	393
wildcard names.....	448
wildcard range command	
usage guidelines.....	394

- window-scale statement.....2175
- window-size statement.....2176
- windows, J-Web, unpredictable results with
  - multiple.....651, 671
- word history
  - operational mode.....455
- working directory
  - current, setting.....519
  - displaying.....531
- world-readable statement
  - archiving of all system log files.....1669
  - system logging.....1696
- write-view statement.....1963
  - usage guidelines.....1856
  
- X**
- XML format
  - displaying command output in.....330
  
- Y**
- yellow alarms.....616, 1237 See minor alarms

