



JUNOS® Software

Administration Guide

Release 9.6

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Revision 01
Published: 2009-07-08

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JUNOS Software Administration Guide

Release 9.6

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

July 2009—Revision 01

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks website at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

About This Guide

xxi

Part 1

Support Overview for Administration Features

Chapter 1	Administration Features on SRX100, SRX210, and SRX240 Services Gateways	3
Chapter 2	Administration Features on SRX650 Services Gateways	9
Chapter 3	Administration Features on SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways	13
Chapter 4	Administration Features on J Series Services Routers	17

Part 2

Configuring the Device for Administration

Chapter 5	User Interface Overview	23
Chapter 6	Configuring Secure Web Access	37
Chapter 7	Managing Administrator Authentication	45
Chapter 8	Setting Up USB Modems for Remote Management	67
Chapter 9	Configuring SNMP for Network Management	85
Chapter 10	Configuring the Device for DHCP	101
Chapter 11	Configuring Autoinstallation	127
Chapter 12	Automating Network Operations and Troubleshooting	135

Part 3

Monitoring the Device

Chapter 13	Monitoring the Device and Routing Operations	147
Chapter 14	Monitoring Events and Managing System Log Files	229
Chapter 15	Configuring and Monitoring Alarms	239

Part 4

Managing Device Software

Chapter 16	Performing Software Upgrades and Reboots	251
Chapter 17	Understanding and Changing Secure and Router Contexts	275
Chapter 18	Configuring Selective Stateless Packet-Based Services	289
Chapter 19	Installing and Managing Licenses	313
Chapter 20	Managing Files	323

Part 5

Diagnosing Performance and Network Problems

Chapter 21	Using Diagnostic Tools	335
------------	------------------------	-----

	Chapter 22	Configuring Packet Capture	381
	Chapter 23	Configuring RPM Probes	395
Part 6	Index		
	Index		423

Table of Contents

	About This Guide	xxi
	J Series and SRX Series Documentation and Release Notes	xxi
	Objectives	xxi
	Audience	xxii
	Supported Routing Platforms	xxii
	How to Use This Manual	xxii
	Document Conventions	xxiv
	Documentation Feedback	xxvi
	Requesting Technical Support	xxvi
Part 1	Support Overview for Administration Features	
Chapter 1	Administration Features on SRX100, SRX210, and SRX240 Services Gateways	3
Chapter 2	Administration Features on SRX650 Services Gateways	9
Chapter 3	Administration Features on SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways	13
Chapter 4	Administration Features on J Series Services Routers	17
Part 2	Configuring the Device for Administration	
Chapter 5	User Interface Overview	23
	User Interface Overview	23
	J-Web Overview	24
	CLI Overview	25
	Before You Begin	25
	Using the J-Web Interface	25
	Starting the J-Web Interface	25
	J-Web Layout	26
	Getting J-Web Help	27

J-Web Sessions	27
.....	27
Using the Command-Line Interface	28
CLI Command Hierarchy	28
Starting the CLI	29
CLI Operational Mode	29
CLI Configuration Mode	30
CLI Basics	31
Editing Keystrokes	31
Command Completion	32
Online Help	33
Configuring the CLI Environment	34

Chapter 6 Configuring Secure Web Access 37

Secure Web Access Terms	37
Secure Web Access Overview	38
Before You Begin	38
Generating SSL Certificates	39
Configuring Management Access	39
Configuring Device Addresses	40
Enabling Access Services	40
Adding, Editing, and Deleting Certificates on the Device	41
Configuring Secure Web Access with a Configuration Editor	42
Verifying Secure Web Access	43
Displaying an SSL Certificate Configuration	43
Displaying a Secure Access Configuration	43

Chapter 7 Managing Administrator Authentication 45

User Authentication Terms	45
User Authentication Overview	46
User Authentication	46
User Accounts	46
Login Classes	47
Permission Bits	47
Denying or Allowing Individual Commands	49
Template Accounts	50
Before You Begin	50
Managing User Authentication	50
Adding a RADIUS Server or TACACS Server for Authentication	50
Configuring System Authentication	51
Adding New Users	51
Managing User Authentication with a Configuration Editor	52
Setting Up RADIUS Authentication	52
Setting Up TACACS+ Authentication	54
Configuring Authentication Order	55

Controlling User Access	56
Defining Login Classes	56
Creating User Accounts	58
Setting Up Template Accounts	59
Creating a Remote Template Account	59
Creating a Local Template Account	60
Securing the Console Port	61
Accessing Remote Devices with the CLI	62
Using the telnet Command	62
Using the ssh Command	63
Configuring Password Retry Limits for Telnet and SSH Access	64
Reverse Telnet	65
Reverse Telnet Overview	65
Reverse Telnet Options	66
Reverse Telnet Restrictions	66
Configuring Reverse Telnet and Reverse SSH	66
CLI Configuration	66

Chapter 8

Setting Up USB Modems for Remote Management 67

USB Modem Terms	67
USB Modem Overview	68
USB Modem Interfaces	68
How the Device Initializes USB Modems	69
USB Modem Connection and Configuration Overview	70
Before You Begin	71
Connecting the USB Modem to the USB Port	71
Configuring USB Modem Interfaces with a Configuration Editor	71
Configuring a USB Modem Interface (Required)	71
Configuring a Dialer Interface (Required)	73
Configuring Dial-In (Required)	74
Configuring CHAP on Dialer Interfaces (Optional)	75
Connecting to the Device from the User End	77
Configuring a Dial-Up Modem Connection at the User End	77
Connecting to the Device from the User End	78
Administering USB Modems	78
Modifying USB Modem Initialization Commands	79
Resetting USB Modems	80
Verifying the USB Modem Configuration	80
Verifying a USB Modem Interface	81
Verifying Dialer Interface Configuration	82

Chapter 9

Configuring SNMP for Network Management 85

SNMP Architecture	85
Management Information Base	86
SNMP Communities	86
SNMP Traps	87

Spoofing SNMP Traps	87
SNMP Health Monitor	87
Before You Begin	88
Configuring SNMP with Quick Configuration	88
Configuring SNMP with a Configuration Editor	93
Defining System Identification Information (Required)	93
Configuring SNMP Agents and Communities (Required)	94
Managing SNMP Trap Groups (Required)	95
Controlling Access to MIBs (Optional)	96
Verifying the SNMP Configuration	97
Verifying SNMP Agent Configuration	97
Verifying SNMP Health Monitor Configuration	98

Chapter 10**Configuring the Device for DHCP****101**

DHCP Terms	101
DHCP Overview	102
DHCP Server Operation	103
DHCP Options	103
Compatibility with Autoinstallation	103
DHCP Client Operation	103
Propagation of TCP/IP Settings	103
DHCP Relay Operation	104
Conflict Detection and Resolution	104
Interface Restrictions	104
Before You Begin	104
Configuring DHCP with Quick Configuration	105
Configuring DHCP Service with Quick Configuration	105
Configuring the Device as a DHCP Client with Quick Configuration	111
Configuring BOOTP or DHCP Relay with Quick Configuration	113
Configuring DHCP with a Configuration Editor	116
Configuring the Device as a DHCP Server	116
Configuring the Device as a DHCP Client	119
Configuring the Device as a DHCP Relay Agent	120
Configuring the Device as a BootP/DHCP Relay Agent	120
Verifying a DHCP Configuration	122
Displaying Global DHCP Information	122
Verifying the DHCP Binding Database	123
Verifying the DHCP Client	124
Verifying DHCP Server Operation	125
Displaying DHCP Relay Statistics	126

Chapter 11**Configuring Autoinstallation****127**

Autoinstallation Terms	127
Autoinstallation Overview	128
Supported Autoinstallation Interfaces and Protocols	128
Typical Autoinstallation Process on a New Device	129
Before You Begin	130

Configuring Autoinstallation with a Configuration Editor	131
Verifying Autoinstallation	133
Verifying Autoinstallation Status	133

Chapter 12**Automating Network Operations and Troubleshooting 135**

Defining and Enforcing Configuration Rules with Commit Scripts	135
Commit Script Overview	135
Enabling Commit Scripts	136
Disabling Commit Scripts	137
Automating Network Management and Troubleshooting with Operation Scripts	138
Operation Script Overview	138
Enabling Operation Scripts	139
Executing Operation Scripts	139
Disabling Operation Scripts	140
Running Self-Diagnostics with Event Policies	140
Event Policy Overview	141
Configuring Event Policies	141

Part 3**Monitoring the Device****Chapter 13****Monitoring the Device and Routing Operations 147**

Monitoring Overview	147
Monitoring Terms	148
Filtering Command Output	148
Monitoring Interfaces	149
Monitoring Events and Alarms	150
Monitoring the System	150
Monitoring System Properties (J Series)	150
Monitoring System Properties (SRX Series)	151
Monitoring Chassis Information	153
IOC to NPC Mapping	155
Monitoring Process Details	156
Monitoring NAT	156
Monitoring Incoming Table Information	156
Monitoring Source NAT Information	157
Monitoring Security Features	158
Monitoring Policies	158
Monitoring Screen Counters	162
Monitoring IDP	164
Monitoring IDP Status	165
Monitoring Flow Session Statistics	166
Monitoring Flow Session Statistics Summary Information	166
Monitoring Flow Information for All Sessions	167
Monitoring Flow Information for Application Sessions	167
Monitoring Flow Session Destination Port Information	168

Monitoring Flow Session Destination Prefix Information	169
Monitoring Flow Session Interface Information	169
Monitoring Flow Session Protocol Information	170
Monitoring Flow Session Resource Manager	170
Monitoring Flow Session Identifier Session	171
Monitoring Flow Session Source Port Information	173
Monitoring Flow Session Source Prefix Information	173
Monitoring Flow Session Tunnel Information	174
Monitoring IDP	174
Monitoring Flow Gate Information	174
Monitoring Firewall Authentication	175
Monitoring Firewall Authentication Table	175
Monitoring Firewall Authentication History	177
Monitoring 802.1x	179
Monitoring ALGs	179
Monitoring SIP ALG Information	180
Monitoring SIP ALG Calls	180
Monitoring SIP ALG Counters	181
Monitoring SIP ALG Rate Information	183
Monitoring SIP ALG Transactions	183
Monitoring H.323 ALG Information	184
Monitoring MGCP ALG Information	185
Monitoring MGCP ALG Calls	185
Monitoring MGCP ALG Counters	186
Monitoring MGCP ALG Endpoints	187
Monitoring SCCP ALG Information	188
Monitoring SCCP ALG Calls	188
Monitoring SCCP ALG Counters	189
Monitoring VPNs	190
Monitoring IKE Gateway Information	190
Monitoring IPsec VPN Information	194
Monitoring Enhanced Switching	198
Monitoring Ethernet Switching	199
Monitoring Spanning Tree	200
Monitoring IGMP Snooping	201
Monitoring GVRP	201
Monitoring Routing Information	202
Monitoring Route Information	202
Monitoring RIP Routing Information	204
Monitoring OSPF Routing Information	204
Monitoring BGP Routing Information	206
Monitoring DLSw Routing Information	207
Monitoring Class-of-Service Performance	208
Monitoring CoS Interfaces	208
Monitoring CoS Classifiers	209
Monitoring CoS Value Aliases	210
Monitoring CoS RED Drop Profiles	210
Monitoring CoS Forwarding Classes	211
Monitoring CoS Rewrite Rules	212
Monitoring CoS Scheduler Maps	213

Monitoring MPLS Traffic Engineering Information	214
Monitoring MPLS Interfaces	215
Monitoring MPLS LSP Information	215
Monitoring MPLS LSP Statistics	216
Monitoring RSVP Session Information	217
Monitoring MPLS RSVP Interfaces Information	218
Monitoring PPPoE	219
Monitoring PPP	222
Monitoring the WAN Acceleration Interface	223
Monitoring Services	223
Monitoring DHCP	223
Monitoring DHCP Service Statistics	223
Monitoring DHCP Client Bindings	224
Monitoring DHCP Conflicts	225
Monitoring DHCP Clients	225
Monitoring DHCP Relay Statistics	226

Chapter 14**Monitoring Events and Managing System Log Files 229**

System Log Message Terms	229
System Log Messages Overview	231
System Log Message Destinations	231
Redundant System Log Server	231
System Log Facilities and Severity Levels	232
Control and Data Plane Logs	233
Before You Begin	233
Configuring System Log Messages with a Configuration Editor	234
Sending System Log Messages to a File	234
Sending System Log Messages to a User Terminal	235
Sending System Log Messages to a Remote Server	235
Archiving System Logs	236
Disabling System Logs	236
Monitoring System Log Messages with the J-Web Event Viewer	236

Chapter 15**Configuring and Monitoring Alarms 239**

Alarm Terms	239
Alarm Overview	240
Alarm Types	240
Alarm Severity	241
Alarm Conditions	241
Interface Alarm Conditions	241
System Alarm Conditions and Corrective Actions	244
Before You Begin	245
Configuring Alarms with a Configuration Editor	245
Checking Active Alarms	247
Verifying the Alarms Configuration	247
Displaying Alarm Configurations	247

Part 4**Managing Device Software****Chapter 16****Performing Software Upgrades and Reboots****251**

Upgrade and Downgrade Overview	252
Upgrade Software Packages	252
Recovery Software Packages	252
Before You Begin	253
Downloading Software Upgrades from Juniper Networks	254
Installing Software Upgrades	254
Installing Software Upgrades with the J-Web Interface	255
Installing Software Upgrades from a Remote Server	255
Installing Software Upgrades by Uploading Files	256
Installing Software Upgrades Using the CLI	257
Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway	259
Prerequisites	259
Setting Environment Variables for BOOTP or DHCP Support	260
Accessing the Loader Prompt	260
Accessing the U-Boot Prompt	260
Installing JUNOS Software Using TFTPBOOT	261
Downgrading the Software	262
Downgrading the Software with the J-Web Interface	262
Downgrading the Software with the CLI	263
Configuring Boot Devices	263
Configuring a Boot Device for Backup with the J-Web Interface	264
Configuring a Boot Device for Backup with the CLI	266
Configuring a Boot Device to Receive Software Failure Memory Snapshots	268
Rebooting or Halting the Device	269
Rebooting or Halting the Device with the J-Web Interface	269
Rebooting the Device with the CLI	271
Halting the Device with the CLI	271
Bringing Chassis Components Online and Offline	272
Chassis Control Restart Options	273

Chapter 17**Understanding and Changing Secure and Router Contexts****275**

Understanding Secure and Router Contexts	275
Secure Context	276
Router Context	276
Secure Context Configuration Settings	276
Router Context Configuration Settings	279
Changing from Secure Context to Router Context	281
Secure-to-Router Context Task Overview	281
Changing to Router Context	283
Changing from Router Context to Secure Context	285
Router-to-Secure Context Task Overview	285

Chapter 18	Configuring Selective Stateless Packet-Based Services	289
	Understanding Packet-Based and Flow-Based Forwarding	289
	Packet-Based Forwarding	290
	Flow-Based Forwarding	290
	Understanding Selective Stateless Packet-Based Services	291
	Related Topics	292
	Configuring Selective Stateless Packet-Based Services	292
	Example: Configuring Selective Stateless Packet-Based Services—End-to-End	
	Packet-Based	294
	CLI Configuration	296
	Related Topics	298
	Verifying the Selective Stateless Packet-Based Services	
	Configuration—End-to-End Packet-Based	298
	Displaying the End-to-End Packet-Based Example Configuration	298
	Verifying Session Establishment On Intranet Traffic	301
	Verifying Session Establishment On Internet Traffic	302
	Example: Configuring Selective Stateless Packet-Based Services—Packet-Based	
	to Flow-Based	303
	CLI Configuration	305
	Related Topics	307
	Verifying the Selective Stateless Packet-Based Services	
	Configuration—Packet-Based to Flow-Based	307
	Displaying the Packet-Based to Flow-Based Example Configuration	307
	Verifying Session Establishment On LAN Traffic	310
	Verifying Session Establishment On Internet Traffic	311
Chapter 19	Installing and Managing Licenses	313
	JUNOS Software Services License Overview	313
	License Enforcement	313
	Software Feature Licenses	314
	License Key Components	314
	Generating a License Key	315
	Managing JUNOS Software Services Licenses with the CLI	315
	Adding New Licenses with the CLI	315
	Deleting a License with the CLI	316
	Updating New Licenses with the CLI	316
	Saving License Keys with the CLI	317
	Managing JUNOS Software Services Licenses with the J-Web Interface	317
	Adding New Licenses with the J-Web Interface	318
	Deleting Licenses with the J-Web Interface	319
	Displaying License Keys with the J-Web interface	319
	Downloading Licenses with the J-Web Interface	319
	Verifying JUNOS Software Services License Management	319
	Displaying Installed Licenses	320
	Displaying License Usage	320
	Displaying Installed License Keys	321

Chapter 20 **Managing Files** **323**

Before You Begin	323
Managing Files with the J-Web Interface	323
Cleaning Up Files	324
Downloading Files	325
Deleting Files	326
Deleting the Backup Software Image	327
Cleaning Up Files with the CLI	328
Managing Accounting Files	328
Encrypting and Decrypting Configuration Files	329
Encrypting Configuration Files	330
Decrypting Configuration Files	331
Modifying the Encryption Key	331

Part 5 **Diagnosing Performance and Network Problems**

Chapter 21 **Using Diagnostic Tools** **335**

Diagnostic Terms	335
Diagnostic Tools Overview	336
J-Web Diagnostic Tools Overview	336
CLI Diagnostic Commands Overview	337
MPLS Connection Checking	339
Before You Begin	341
General Preparation	341
Ping MPLS Preparation	341
MPLS Enabled	341
Loopback Address	341
Source Address for Probes	341
Pinging Hosts from the J-Web Interface	341
Using the J-Web Ping Host Tool	342
Ping Host Results and Output Summary	344
Checking MPLS Connections from the J-Web Interface	345
Using the J-Web Ping MPLS Tool	346
Ping MPLS Results and Output	349
Tracing Unicast Routes from the J-Web Interface	350
Using the J-Web Traceroute Tool	351
Traceroute Results and Output Summary	353
Capturing and Viewing Packets with the J-Web Interface	354
Using J-Web Packet Capture	354
Packet Capture Results and Output Summary	357
Using CLI Diagnostic Commands	359
Pinging Hosts from the CLI	359
Checking MPLS Connections from the CLI	361
Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs	362
Pinging Layer 3 VPNs	363

Pinging Layer 2 VPNs	363
Pinging Layer 2 Circuits	365
Tracing Unicast Routes from the CLI	365
Using the traceroute Command	366
Using the traceroute monitor Command	367
Tracing Multicast Routes from the CLI	369
Using the mtrace from-source Command	370
Using the mtrace monitor Command	372
Displaying Log and Trace Files from the CLI	373
Monitoring Interfaces and Traffic from the CLI	373
Using the monitor interface Command	373
Using the monitor traffic Command	375

Chapter 22**Configuring Packet Capture****381**

Packet Capture Terms	381
Packet Capture Overview	382
Packet Capture on Device Interfaces	383
Firewall Filters for Packet Capture	384
Packet Capture Files	384
Analysis of Packet Capture Files	384
Before You Begin	385
Configuring Packet Capture with a Configuration Editor	385
Enabling Packet Capture (Required)	385
Configuring Packet Capture on an Interface (Required)	387
Configuring a Firewall Filter for Packet Capture (Optional)	388
Disabling Packet Capture	389
Deleting Packet Capture Files	389
Changing Encapsulation on Interfaces with Packet Capture Configured	390
Verifying Packet Capture	391
Displaying a Packet Capture Configuration	391
Displaying a Firewall Filter for Packet Capture Configuration	392
Verifying Captured Packets	392

Chapter 23**Configuring RPM Probes****395**

RPM Terms	395
RPM Overview	396
RPM Probes	396
RPM Tests	397
Probe and Test Intervals	397
Jitter Measurement with Hardware Timestamping	397
RPM Statistics	398
RPM Thresholds and Traps	399
RPM for BGP Monitoring	399
Before You Begin	399
Configuring RPM with Quick Configuration	400
Configuring RPM with a Configuration Editor	406
Configuring Basic RPM Probes	406
Configuring TCP and UDP Probes	409

Tuning RPM Probes	411
Configuring RPM Probes to Monitor BGP Neighbors	412
Configuring RPM Probes for BGP Monitoring	413
Directing RPM Probes to Select BGP Routers	414
Verifying an RPM Configuration	415
Verifying RPM Services	415
Verifying RPM Statistics	416
Verifying RPM Probe Servers	417
Monitoring RPM Probes	418

Part 6

Index

Index	423
-------------	-----

About This Guide

This preface provides the following guidelines for using the *JUNOS Software Administration Guide*:

- J Series and SRX Series Documentation and Release Notes on page xxi
- Objectives on page xxi
- Audience on page xxii
- Supported Routing Platforms on page xxii
- How to Use This Manual on page xxii
- Document Conventions on page xxiv
- Documentation Feedback on page xxvi
- Requesting Technical Support on page xxvi

J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see
<http://www.juniper.net/techpubs/software/junos-jseries/index-main.html> .

For a list of related SRX Series documentation, see
<http://www.juniper.net/techpubs/hardware/srx-series-main.html>.

If the information in the latest release notes differs from the information in the documentation, follow the *SRX Series Software 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/>.

Objectives

This guide contains instructions for managing users and operations, monitoring network performance, upgrading software, and diagnosing common problems on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J Series Services Router or an SRX Series Services Gateway running JUNOS Software. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running JUNOS Software.

How to Use This Manual

This manual and the other manuals in this set explain how to install, configure, and manage:

- JUNOS Software for J Series Services Routers
- JUNOS Software for SRX Series Services Gateways

Table 1 on page xxii identifies the tasks required to configure and manage these devices and shows where to find task information and instructions.

Table 1: Tasks and Related Documentation

Task	Related Documentation
Basic Device Installation and Setup	
■ Reviewing safety warnings and compliance statements	J Series Services Routers:
■ Installing hardware and establishing basic connectivity	■ <i>J Series Services Routers Quick Start</i>
■ Initially setting up a device	■ <i>J Series Services Routers Hardware Guide</i>
	■ <i>JUNOS Software Release Notes</i>
	SRX Series Services Gateways: the appropriate <i>Services Gateway Getting Started Guide</i>
Migration from ScreenOS or JUNOS Software (Legacy Services) to JUNOS Software (if necessary)	
■ Migrating from JUNOS Software (legacy services) Release 8.3 or later to JUNOS Software	<i>JUNOS Software Migration Guide</i> (J Series Services Routers only)
■ Migrating from ScreenOS Release 5.4 or later to JUNOS Software.	
Context—Changing to Secure Context or Router Context	

Table 1: Tasks and Related Documentation *(continued)*

Task	Related Documentation
Changing the device from one context to another and understanding the factory default settings	<i>JUNOS Software Administration Guide</i>
Interface Configuration	
Configuring device interfaces	<ul style="list-style-type: none"> ■ <i>JUNOS Software Interfaces and Routing Configuration Guide</i> ■ <i>JUNOS Software CLI Reference</i>
Deployment Planning and Configuration	
<ul style="list-style-type: none"> ■ Understanding and gathering information required to design network firewalls and IPsec VPNs ■ Implementing a JUNOS Software firewall from a sample scenario ■ Implementing a policy-based IPsec VPN from a sample scenario 	<i>JUNOS Software Design and Implementation Guide</i> (J Series Services Routers only)
Security Configuration	
Configuring and managing the following security services:	<ul style="list-style-type: none"> ■ <i>JUNOS Software Security Configuration Guide</i> ■ <i>JUNOS Software CLI Reference</i>
<ul style="list-style-type: none"> ■ Stateful firewall policies ■ Zones and their interfaces and address books ■ IPsec VPNs ■ Firewall screens ■ Interface modes: Network Address Translation (NAT) mode and Router mode ■ Public Key Cryptography (PKI) ■ Application Layer Gateways (ALGs) ■ Chassis clusters ■ Intrusion Detection and Prevention (IDP) 	
Routing Protocols and Services Configuration	
<ul style="list-style-type: none"> ■ Configuring routing protocols, including static routes and the dynamic routing protocols RIP, OSPF, BGP, and IS-IS ■ Configuring class-of-service (CoS) features, including traffic shaping and policing ■ Configuring packet-based stateless firewall filters (access control lists) to control access and limit traffic rates ■ Configuring MPLS to control network traffic patterns 	<ul style="list-style-type: none"> ■ <i>JUNOS Software Interfaces and Routing Configuration Guide</i> ■ <i>JUNOS Software CLI Reference</i>
WAN Acceleration Module Installation (Optional)	
Installing and initially configuring a WXC Integrated Services Module (ISM 200)	<i>WXC Integrated Services Module Installation and Configuration Guide</i> (J Series Services Routers only)
User and System Administration	

Table 1: Tasks and Related Documentation *(continued)*

Task	Related Documentation	
<ul style="list-style-type: none">■ Administering user authentication and access■ Monitoring the device, routing protocols, and routing operations■ Configuring and monitoring system alarms and events, real-time performance (RPM) probes, and performance■ Monitoring the firewall and other security-related services■ Managing system log files■ Upgrading software■ Diagnosing common problems	<i>JUNOS Software Administration Guide</i>	
User Interfaces		
<ul style="list-style-type: none">■ Understanding and using the J-Web interface■ Understanding and using the CLI configuration editor	<ul style="list-style-type: none">■ <i>J Series Services Routers Quick Start</i> (J Series Services Routers only)■ <i>JUNOS Software Administration Guide</i>	

Document Conventions

Table 2 on page xxiv defines the notice icons used in this guide.

Table 2: 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.

Table 3 on page xxv defines the text and syntax conventions used in this guide.

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>JUNOS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name domain-name
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the <code>stub</code> statement at the [edit <code>protocols ospf area area-id</code>] hierarchy level. The console port is labeled <code>CONSOLE</code>.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

Table 3: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for Network Operations Guides [NOGs])

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 JNASC support contract, or are covered under warranty, and need postsales 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/customers/support/downloads/710059.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: <https://www.juniper.net/alerts/>
- 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 located at <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, visit us at <http://www.juniper.net/support/requesting-support.html>.

Part 1

Support Overview for Administration Features

- Administration Features on SRX100, SRX210, and SRX240 Services Gateways on page 3
- Administration Features on SRX650 Services Gateways on page 9
- Administration Features on SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways on page 13
- Administration Features on J Series Services Routers on page 17

Chapter 1

Administration Features on SRX100, SRX210, and SRX240 Services Gateways

The following tables list administration features that are supported on the SRX100, SRX210, and SRX240 Services Gateways.

Table 4: Administrator Authentication

Feature	More Information
RADIUS	"User Authentication Overview" on page 46
TACACS +	"User Authentication Overview" on page 46
Local authentication	"User Authentication Overview" on page 46

Table 5: Alarms

Feature	More Information
Chassis alarms	"Alarm Types" on page 240
Interface alarms	"Alarm Types" on page 240
System alarms	"Alarm Types" on page 240

Table 6: Autoinstallation

Feature	More Information
Autoinstallation	"Autoinstallation Overview" on page 128

The following table applies only to the SRX240 Services Gateway.

Table 7: Chassis Management

Feature	More Information
Chassis management	“Monitoring Chassis Information” on page 153 <i>JUNOS Software Interfaces and Routing Configuration Guide</i>

Table 8: DHCP

Feature	More Information
Dynamic Host Configuration Protocol (DHCP) server address pools	“DHCP Server Operation” on page 103
DHCP server static mapping	“DHCP Server Operation” on page 103
DHCP client	“DHCP Client Operation” on page 103
DHCP server	“DHCP Server Operation” on page 103
DHCP relay agent	“DHCP Relay Operation” on page 104

Table 9: Diagnostic Tools

Feature	More Information
Ping host	“J-Web Diagnostic Tools Overview” on page 336
Ping MPLS	“MPLS Enabled” on page 341
Traceroute	“J-Web Diagnostic Tools Overview” on page 336
CLI terminal	“CLI Diagnostic Commands Overview” on page 337
J-flow version 8	JUNOS J-Web Interface User Guide

Table 10: File Management Options

Feature	More Information
Clean up unnecessary files	“Cleaning Up Files” on page 324
Delete individual files	“Deleting Files” on page 326
Delete backup software image	“Deleting the Backup Software Image” on page 327
Download system files	“Downloading Files” on page 325
Encrypt/decrypt configuration files (SRX240 only)	“Encrypting and Decrypting Configuration Files” on page 329
Manage account files (SRX240 only)	“Managing Accounting Files” on page 328

Table 11: Network Operations and Troubleshooting Automation

Feature	More Information
Extensible Stylesheet Language Transformations (XSLT) commit scripts	“Commit Script Overview” on page 135
Operation scripts	“Operation Script Overview” on page 138
Event policies	“Event Policy Overview” on page 141

Table 12: Packet Capture Options

Feature	More Information
Packet capture	“Packet Capture Overview” on page 382

Table 13: RPM Probe Options

Feature	More Information
Real-time performance monitoring (RPM)	“Configuring RPM Probes” on page 395

Table 14: Secure and Router Context Options

Feature	More Information
Secure context	“Secure Context” on page 276
Router context	“Understanding and Changing Secure and Router Contexts” on page 275
Selective stateless packet-based services	“Configuring Selective Stateless Packet-Based Services” on page 289

Table 15: Secure Web Access

Feature	More Information
Certificate authorities (CAs)	“Secure Web Access Overview” on page 38
Hypertext Transfer Protocol (HTTP)	“Secure Web Access Overview” on page 38

Table 16: SNMP Network Management

Feature	More Information
SNMP v1, v2, v3	“SNMP Architecture” on page 85

Table 17: System Log Files

Feature	More Information
Configuring system log messages	“Configuring System Log Messages with a Configuration Editor” on page 234
Sending system log messages to a file	“Sending System Log Messages to a File” on page 234
Sending system log messages to a user terminal	“Sending System Log Messages to a User Terminal” on page 235
Archiving system logs	“Archiving System Logs” on page 236
Disabling system logs	“Disabling System Logs” on page 236
Viewing system log messages	“Monitoring System Log Messages with the J-Web Event Viewer” on page 236
Viewing data plane logs	“Control and Data Plane Logs” on page 233

Table 18: Upgrade and Reboot Options

Feature	More Information
Software upgrades and downgrades	“Upgrade and Downgrade Overview” on page 252
Boot device configuration	“Configuring Boot Devices” on page 263
Boot device recovery	“Recovery Software Packages” on page 252
Chassis components control	“Bringing Chassis Components Online and Offline” on page 272
Chassis restart	“Chassis Control Restart Options” on page 273
TFTPBOOT Installation (SRX100 and SRX210 only)	“Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway” on page 259

Table 19: USB Modem Remote Management

Feature	More Information
Universal serial bus (USB) modem support	“USB Modem Overview” on page 68

Table 20: User Interfaces

Feature	More Information
J-Web user interface	“J-Web Overview” on page 24
Command-line interface (CLI)	“CLI Overview” on page 25

Table 20: User Interfaces *(continued)*

Feature	More Information
Network and Security Manager (NSM)	<i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>
JUNOScope application	<i>JUNOScope Software User Guide</i>
JUNOScript	<i>JUNOScript API Guide</i>
Session and Resource Control (SRC) application	<i>SRC-PE Getting Started Guide</i>

Chapter 2

Administration Features on SRX650 Services Gateways

The following tables list administration features that are supported on the SRX650 Services Gateways.

Table 21: Administrator Authentication

Feature	More Information
RADIUS	“User Authentication Overview” on page 46
TACACS +	“User Authentication Overview” on page 46
Local authentication	“User Authentication Overview” on page 46

Table 22: Alarms

Feature	More Information
Chassis alarms	“Alarm Types” on page 240
Interface alarms	“Alarm Types” on page 240
System alarms	“Alarm Types” on page 240

Table 23: Autoinstallation

Feature	More Information
Autoinstallation	“Autoinstallation Overview” on page 128

Table 24: Chassis Management

Feature	More Information
Chassis management	“Monitoring Chassis Information” on page 153 <i>JUNOS Software Interfaces and Routing Configuration Guide</i>

Table 25: DHCP

Feature	More Information
Dynamic Host Configuration Protocol (DHCP) server address pools	“DHCP Server Operation” on page 103
DHCP server static mapping	“DHCP Server Operation” on page 103
DHCP client	“DHCP Client Operation” on page 103
DHCP server	“DHCP Server Operation” on page 103
DHCP relay agent	“DHCP Relay Operation” on page 104

Table 26: Diagnostic Tools

Feature	More Information
Ping host	“J-Web Diagnostic Tools Overview” on page 336
Ping MPLS	“MPLS Enabled” on page 341
Traceroute	“J-Web Diagnostic Tools Overview” on page 336
CLI terminal	“CLI Diagnostic Commands Overview” on page 337
J-flow version 8	

Table 27: File Management Options

Feature	More Information
Clean up unnecessary files	“Cleaning Up Files” on page 324
Delete individual files	“Deleting Files” on page 326
Delete backup software image	“Deleting the Backup Software Image” on page 327
Download system files	“Downloading Files” on page 325
Encrypt/decrypt configuration files	“Encrypting and Decrypting Configuration Files” on page 329
Manage account files	“Managing Accounting Files” on page 328

Table 28: Network Operations and Troubleshooting Automation

Feature	More Information
Extensible Stylesheet Language Transformations (XSLT) commit scripts	“Commit Script Overview” on page 135
Operation scripts	“Operation Script Overview” on page 138
Event policies	“Event Policy Overview” on page 141

Table 29: RPM Probe Options

Feature	More Information
Real-time performance monitoring (RPM)	“Configuring RPM Probes” on page 395

Table 30: Secure and Router Context Options

Feature	More Information
Secure context	“Secure Context” on page 276
Router context	“Understanding and Changing Secure and Router Contexts” on page 275
Selective stateless packet-based services	“Configuring Selective Stateless Packet-Based Services” on page 289

Table 31: Secure Web Access

Feature	More Information
Certificate authorities (CAs)	“Secure Web Access Overview” on page 38
Hypertext Transfer Protocol (HTTP)	“Secure Web Access Overview” on page 38

Table 32: System Log Files

Feature	More Information
Configuring system log messages	“Configuring System Log Messages with a Configuration Editor” on page 234
Sending system log messages to a file	“Sending System Log Messages to a File” on page 234
Sending system log messages to a user terminal	“Sending System Log Messages to a User Terminal” on page 235
Archiving system logs	“Archiving System Logs” on page 236
Disabling system logs	“Disabling System Logs” on page 236
Viewing system log messages	“Monitoring System Log Messages with the J-Web Event Viewer” on page 236
Viewing data plane logs	“Control and Data Plane Logs” on page 233

Table 33: Upgrade and Reboot Options

Feature	More Information
Software upgrades and downgrades	“Upgrade and Downgrade Overview” on page 252

Table 33: Upgrade and Reboot Options *(continued)*

Feature	More Information
Boot device configuration	“Configuring Boot Devices” on page 263
Boot device recovery	“Recovery Software Packages” on page 252
Chassis components control	“Bringing Chassis Components Online and Offline” on page 272
Chassis restart	“Chassis Control Restart Options” on page 273
TFTPBOOT Installation	“Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway” on page 259

Table 34: User Interfaces

Feature	More Information
J-Web user interface	“J-Web Overview” on page 24
Command-line interface (CLI)	“CLI Overview” on page 25
Network and Security Manager (NSM)	<i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>
JUNOScope application	<i>JUNOScope Software User Guide</i>
JUNOScript	<i>JUNOScript API Guide</i>

Chapter 3

Administration Features on SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways

The following tables list administration features that are supported on the SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways.

Table 35: Administrator Authentication

Feature	More Information
RADIUS	“User Authentication Overview” on page 46
TACACS +	“User Authentication Overview” on page 46
Local authentication (SRX5600 and SRX5800 only)	“User Authentication Overview” on page 46

Table 36: Alarms

Feature	More Information
Chassis alarms	“Alarm Types” on page 240
Interface alarms	“Alarm Types” on page 240
System alarms	“Alarm Types” on page 240

Table 37: Chassis Management

Feature	More Information
Chassis management	“Monitoring Chassis Information” on page 153 <i>JUNOS Software Interfaces and Routing Configuration Guide</i>

Table 38: DHCP

Feature	More Information
Dynamic Host Configuration Protocol (DHCP) server address pools	“DHCP Server Operation” on page 103
DHCP server static mapping	“DHCP Server Operation” on page 103
DHCP client	“DHCP Client Operation” on page 103
DHCP server	“DHCP Server Operation” on page 103
DHCP relay agent	“DHCP Relay Operation” on page 104

Table 39: Diagnostic Tools

Feature	More Information
Ping host	“J-Web Diagnostic Tools Overview” on page 336
Traceroute	“J-Web Diagnostic Tools Overview” on page 336
CLI terminal	“CLI Diagnostic Commands Overview” on page 337

Table 40: File Management Options

Feature	More Information
Clean up unnecessary files	“Cleaning Up Files” on page 324
Delete individual files	“Deleting Files” on page 326
Delete backup software image	“Deleting the Backup Software Image” on page 327

Table 41: Network Operations and Troubleshooting Automation

Feature	More Information
Extensible Stylesheet Language Transformations (XSLT) commit scripts	“Commit Script Overview” on page 135
Operation scripts	“Operation Script Overview” on page 138
Event policies	“Event Policy Overview” on page 141

Table 42: Secure Web Access

Feature	More Information
Certificate authorities (CAs)	“Secure Web Access Overview” on page 38
Hypertext Transfer Protocol (HTTP)	“Secure Web Access Overview” on page 38

Table 43: SNMP Network Management

Feature	More Information
SNMP v1, v2, v3	“SNMP Architecture” on page 85

Table 44: System Log Files

Feature	More Information
Configuring system log messages	“Configuring System Log Messages with a Configuration Editor” on page 234
Sending system log messages to a file	“Sending System Log Messages to a File” on page 234
Sending system log messages to a user terminal	“Sending System Log Messages to a User Terminal” on page 235
Archiving system logs	“Archiving System Logs” on page 236
Disabling system logs	“Disabling System Logs” on page 236
Viewing system log messages	“Monitoring System Log Messages with the J-Web Event Viewer” on page 236
Viewing data plane logs	“Control and Data Plane Logs” on page 233
Multiple system log servers	“Redundant System Log Server” on page 231

Table 45: Upgrade and Reboot Options

Feature	More Information
Software upgrades and downgrades	“Upgrade and Downgrade Overview” on page 252
Boot device configuration	“Configuring Boot Devices” on page 263
Boot device recovery	“Recovery Software Packages” on page 252
Chassis components control	“Bringing Chassis Components Online and Offline” on page 272
Chassis restart	“Chassis Control Restart Options” on page 273

Table 46: User Interfaces

Feature	More Information
J-Web user interface	“J-Web Overview” on page 24
Command-line interface (CLI) configuration editor	“CLI Overview” on page 25
Network and Security Manager (NSM)	<i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>

Table 46: User Interfaces *(continued)*

Feature	More Information
JUNOScope application	<i>JUNOScope Software User Guide</i>
JUNOScript	<i>JUNOScript API Guide</i>

Chapter 4

Administration Features on J Series Services Routers

The following tables list administration features that are supported on J Series Services Routers.

Table 47: Accessing Remote Devices with the CLI

Feature	More Information
Reverse Telnet	“Reverse Telnet” on page 65

Table 48: Administrator Authentication

Feature	More Information
RADIUS	“User Authentication Overview” on page 46
TACACS +	“User Authentication Overview” on page 46
Local authentication	“User Authentication Overview” on page 46

Table 49: Alarms

Feature	More Information
Chassis alarms	“Alarm Types” on page 240
Interface alarms	“Alarm Types” on page 240
System alarms	“Alarm Types” on page 240

Table 50: Autoinstallation

Feature	More Information
Autoinstallation	“Autoinstallation Overview” on page 128

Table 51: DHCP

Feature	More Information
Dynamic Host Configuration Protocol (DHCP) server address pools	“DHCP Server Operation” on page 103
DHCP server static mapping	“DHCP Server Operation” on page 103
DHCP client	“DHCP Client Operation” on page 103
DHCP server	“DHCP Server Operation” on page 103
DHCP relay agent	“DHCP Relay Operation” on page 104

Table 52: Diagnostic Tools

Feature	More Information
Ping host	“J-Web Diagnostic Tools Overview” on page 336
Ping MPLS	“J-Web Diagnostic Tools Overview” on page 336
Traceroute	“J-Web Diagnostic Tools Overview” on page 336
CLI terminal	“CLI Diagnostic Commands Overview” on page 337
J-flow version 8	

Table 53: File Management Options

Feature	More Information
Clean up unnecessary files	“Cleaning Up Files” on page 324
Download system files	“Downloading Files” on page 325
Delete individual files	“Deleting Files” on page 326
Delete backup software image	“Deleting the Backup Software Image” on page 327
Manage account files	“Managing Accounting Files” on page 328
Encrypt/decrypt configuration files	“Encrypting and Decrypting Configuration Files” on page 329

Table 54: Network Operations and Troubleshooting Automation

Feature	More Information
Extensible Stylesheet Language Transformations (XSLT) commit scripts	“Commit Script Overview” on page 135
Operation scripts	“Operation Script Overview” on page 138
Event policies	“Event Policy Overview” on page 141

Table 55: Packet Capture Options

Feature	More Information
Packet capture	“Packet Capture Overview” on page 382

Table 56: RPM Probe Options

Feature	More Information
Real-time performance monitoring (RPM)	“RPM Overview” on page 396

Table 57: Secure and Router Context Options

Feature	More Information
Secure context	“Secure Context” on page 276
Router context	“Router Context” on page 276
Selective stateless packet-based services	“Configuring Selective Stateless Packet-Based Services” on page 289

Table 58: Secure Web Access

Feature	More Information
Certificate authorities (CAs)	“Secure Web Access Overview” on page 38
Hypertext Transfer Protocol (HTTP)	“Secure Web Access Overview” on page 38

Table 59: SNMP Network Management

Feature	More Information
SNMP v1, v2, v3	“SNMP Architecture” on page 85

Table 60: System Log Files

Feature	More Information
Configuring system log messages	“Configuring System Log Messages with a Configuration Editor” on page 234
Sending system log messages to a file	“Sending System Log Messages to a File” on page 234
Sending system log messages to a user terminal	“Sending System Log Messages to a User Terminal” on page 235
Archiving system logs	“Archiving System Logs” on page 236

Table 60: System Log Files *(continued)*

Feature	More Information
Disabling system logs	“Disabling System Logs” on page 236
Viewing system log messages	“Monitoring System Log Messages with the J-Web Event Viewer” on page 236
Viewing data plane logs	“Control and Data Plane Logs” on page 233

Table 61: Upgrade and Reboot Options

Feature	More Information
Software upgrades and downgrades	“Upgrade and Downgrade Overview” on page 252
Boot device configuration	“Configuring Boot Devices” on page 263
Boot device recovery	“Recovery Software Packages” on page 252
Chassis components control	“Bringing Chassis Components Online and Offline” on page 272
Chassis restart	“Chassis Control Restart Options” on page 273

Table 62: USB Modem Remote Management

Feature	More Information
Universal serial bus (USB) modem support	“USB Modem Overview” on page 68

Table 63: User Interfaces

Feature	More Information
J-Web user interface	“J-Web Overview” on page 24
Command-line interface (CLI) configuration editor	“CLI Overview” on page 25
Network and Security Manager (NSM)	<i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i>
JUNOScope application	<i>JUNOScope Software User Guide</i>
JUNOScript	<i>JUNOScript API Guide</i>
Session and Resource Control (SRC) application	<i>SRC-PE Getting Started Guide</i>

Part 2

Configuring the Device for Administration

- User Interface Overview on page 23
- Configuring Secure Web Access on page 37
- Managing Administrator Authentication on page 45
- Setting Up USB Modems for Remote Management on page 67
- Configuring SNMP for Network Management on page 85
- Configuring the Device for DHCP on page 101
- Configuring Autoinstallation on page 127
- Automating Network Operations and Troubleshooting on page 135

Chapter 5

User Interface Overview

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



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 JUNOScope and Session and Resource Control (SRC) applications. For more information about these products, see the *JUNOScope Software User Guide* and the *SRC-PE Getting Started Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- User Interface Overview on page 23
- Before You Begin on page 25
- Using the J-Web Interface on page 25
- J-Web Sessions on page 27
- Using the Command-Line Interface on page 28

User Interface Overview

This section contains the following topics:

- J-Web Overview on page 24
- CLI Overview on page 25

You can operate the device either in secure or router context. With the J-Web interface and the command-line interface (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.

For information about secure and router contexts, see “Understanding Secure and Router Contexts” on page 275.

J-Web Overview

The J-Web 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 interface:

- **Dashboard (SRX Series devices only)** — Displays a high-level details of Chassis View, system identification, resource utilization, security resources, system alarms, file usage, login sessions, chassis status, and storage usage.
- **Monitoring** — Displays 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 device, and manage configuration files. The J-Web interface provides the following different configuration methods:
 - Configure the device quickly and easily without configuring each statement individually.
 - Edit a graphical version of the JUNOS Software 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.

- **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.
- **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.
- **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.

For more information about the J-Web interface, see “Using the J-Web Interface” on page 25.

CLI Overview

The CLI is a straightforward command 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 guide refers to configuration mode as the *CLI configuration editor*.

For more information about the CLI, see “Using the Command-Line Interface” on page 28.

Before You Begin

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.

Using the J-Web Interface

This section contains the following topics:

- Starting the J-Web Interface on page 25
- J-Web Layout on page 26
- Getting J-Web Help on page 27

For more information about using the J-Web interface, see the *J-Web Interface User Guide*.

Starting the J-Web Interface

To start the J-Web 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 Software 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. After typing **http://** or **https://** in your Web browser, type the hostname or IP address of the device and press Enter.

The J-Web login page appears.

3. On the login page, type your username and password, and click **Log In**.

To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.



NOTE: The default username is **root** with no password. You must change this during initial configuration or the system does not accept the configuration.

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane.

J-Web 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.
- Help—A link to context-sensitive Help information is available in the upper-right corner.
- About—A link to information about the J-Web interface, such as the version number, is available in the upper-right corner.
- 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 J-Web task to access it.
 - **Dashboard**— Displays the information of the system.
 - **Configure**—Configure the device and view configuration history.
 - **Monitor**—View information about configuration and hardware on the device.
 - **Maintain**—Manage files and licenses, upgrade software, and reboot the device.
 - **Troubleshoot**—Troubleshoot network connectivity problems.

The main pane of the J-Web user interface includes the following elements to help you configure the device:

- Red asterisk (*)—A red asterisk is displayed next to all required fields.

- **Help (?) icon**—The 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.

Getting J-Web Help

To get Help in the J-Web 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. 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 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.

J-Web Sessions

This section explains how J-Web sessions are established.

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 Software. 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 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.

Using the Command-Line Interface

This section contains the following topics:

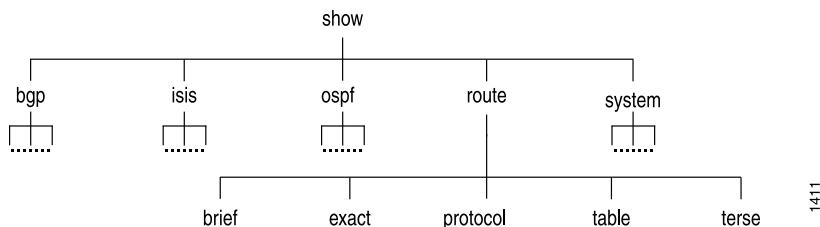
- CLI Command Hierarchy on page 28
- Starting the CLI on page 29
- CLI Operational Mode on page 29
- CLI Configuration Mode on page 30
- CLI Basics on page 31

For more information about the CLI, see the *JUNOS CLI User Guide*.

CLI Command Hierarchy

The CLI commands 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 device system and system software are grouped under the **show** command, and all commands that display information about the routing table are grouped under the **show route** command. Figure 1 on page 28 illustrates a portion of the **show** command hierarchy.

Figure 1: CLI Command Hierarchy Example



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**.

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. If you type

a partial command name followed immediately by a question mark (with no intervening space), you see a list of commands that match the partial name you typed.

Starting the CLI

To start the CLI:

1. Establish a connection with the device:
 - To access the device remotely from the network, enter the command you typically use to establish a remote connection (such as **Telnet** or **ssh**) using the device hostname.
 - To access the device through a management device attached to the console port, start the terminal application.
 - To access the device through the J-Web interface, select **Troubleshoot > CLI Terminal** in the J-Web interface. For more information, see the *J-Web Interface User Guide*.
2. Log in using your username and password.

After you log in, you enter a UNIX shell.

3. Start the CLI.

```
% cli
user@host>
```

The presence of the angle bracket (>) prompt indicates the CLI has started. By default, the prompt is preceded by a string that contains your username and the hostname of the router.

To exit the CLI and return to the UNIX shell, enter the **quit** command.

CLI Operational Mode

The CLI has two modes: *operational* and *configuration*. When you log in to the device and the CLI starts, you are at the top level of operational mode.

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
monitor        Show real-time debugging information
mtrace         Trace multicast path from source to receiver
ping           Ping remote target
quit           Exit the management session
request        Make system-level requests
```

restart	Restart software process
set	Set CLI properties, date/time, craft interface message
show	Show system information
ssh	Start secure shell on another host
start	Start shell
telnet	Telnet to another host
test	Perform diagnostic debugging
traceroute	Trace route to remote host

At the top level of operational mode are a number of broad groups of CLI commands that are used to perform the following functions:

- Control the CLI environment.
- Monitor and troubleshoot the device.
- Connect to other systems.
- Manage files and software images.
- Control software processes.
- Stop and reboot the device.
- Enter configuration mode.

To control the CLI environment, see “Configuring the CLI Environment” on page 34. To enter configuration mode, see “CLI Configuration Mode” on page 30. For information about the other CLI operational mode functions, see the *JUNOS Software Administration Guide*.

CLI Configuration Mode

To configure the device, including system parameters, routing protocols, security, interfaces, network management, and user access, you must enter configuration mode. In configuration mode, the CLI provides commands to configure the device, load a text (ASCII) file that contains the device configuration, activate a configuration, and save the configuration to a text file.

You enter configuration mode by entering the `configure` operational mode command. The CLI prompt changes from `user@host>` to `user@host#`.

To view a list of configuration mode commands, type a question mark (?) at the command-line prompt. (You do not need to press Enter after typing the question mark.)

```

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
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

The JUNOS software configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which contain other statements, and *leaf statements*, which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.

Each statement consists of a fixed keyword and, optionally, an identifier that you define, such as the name of an interface or a username.

To configure the device or to modify an existing configuration, you add statements to the configuration with the **edit** and **set** configuration mode commands. For more information about the CLI configuration editor and configuration mode, see the JUNOS Software configuration guides.

CLI Basics

This section contains the following topics:

- Editing Keystrokes on page 31
- Command Completion on page 32
- Online Help on page 33
- Configuring the CLI Environment on page 34

Editing Keystrokes

In the CLI, you use keystrokes to move around on and edit the command line, and to scroll through a list of recently executed commands. Table 64 on page 32 lists some typical CLI editing tasks and the keystrokes that perform them.

Table 64: CLI Editing Keystrokes

Task Category	Action	Keyboard Sequence
Move the cursor.	Move the cursor back one character.	Ctrl-b
	Move the cursor back one word.	Esc b
	Move the cursor forward one character.	Ctrl-f
	Move the cursor forward one word.	Esc f
	Move the cursor to the end of the command line.	Ctrl-e
Delete characters.	Delete the character before the cursor.	Ctrl-h, Delete, or Backspace
	Delete the character at the cursor.	Ctrl-d
	Delete all characters from the cursor to the end of the command line.	Ctrl-k
	Delete all characters on the command line.	Ctrl-u or Ctrl-x
	Delete the word before the cursor.	Ctrl-w or Esc Backspace
	Delete the word after the cursor.	Esc 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 /
Repeat keyboard sequences.	Specify the number of times to execute a keyboard sequence. Replace <i>number</i> with a number from 1 through 9, and replace <i>sequence</i> with a keyboard sequence in this table.	Esc <i>number sequence</i>

Command Completion

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 Spacebar. If the partially typed letters uniquely identify a command, the complete command name appears. Otherwise, a message indicates that your entry is ambiguous or invalid. Possible command completions are displayed if your entry is ambiguous.

You can also use command completion on filenames and usernames. To display all possible values, type one or more characters followed immediately by a question mark. To complete these partial entries, press Tab only. Pressing Spacebar does not work.

Online Help

The CLI provides context-sensitive Help at every level of the command hierarchy. The Help information tells you which commands are available at the current level in the hierarchy and provides a brief description of each.

To get help while in the CLI, type a question mark (?) in one of the following ways:

- Type a question mark at the command-line prompt. The CLI lists the available commands and options. For examples, see “CLI Operational Mode” on page 29 and “CLI Configuration Mode” on page 30.
- Type a question mark after entering the complete name of a command or command option. The CLI lists the available commands and options, then redisplay the command names and options that you typed:

```
user@host# set schedulers ?

regress@arcona# set schedulers ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
> scheduler             Scheduler configuration
[edit]
user@host# set schedulers
```

- Type a question mark in the middle of a command name. The CLI lists possible command completions that match the letters you have entered so far, then redisplay the letters that you typed. For example, to list all operational mode commands that start with the letter s, type the following:

```
user@host> s?

Possible completions:
set          Set CLI properties, date/time, craft interface message
show        Show system information
ssh         Start secure shell on another host
start       Start shell
```

When you enter the **help** commands described in Table 65 on page 34, the CLI displays usage guidelines and summary information for configuration statements and operational mode commands. You can enter **help** commands in operational or configuration mode.

Table 65: help Commands

CLI Command	Description
<code>help apropos <i>string</i></code>	<p>Displays Help based on a text string contained in a statement or command name.</p> <p>If the string contains spaces, enclose it in quotation marks. You also can specify a regular expression for the string, using standard UNIX-style regular expression syntax.</p> <p>In configuration mode, this command displays statement names and Help text that match the string specified.</p> <p>In operational mode, this command displays the following types of commands that match the string specified, plus Help text:</p> <ul style="list-style-type: none"> ■ Operational mode commands ■ <code>help topic</code> and <code>help reference</code> commands you can enter for more information <p>For example, to get a list of statements that contain the string <code>traps</code>, enter the <code>help apropos traps</code> command in configuration mode.</p>
<code>help reference <i>string</i></code>	<p>Displays summary information for configuration statements.</p> <p>For example, to display summary information for the OSPF hello interval, enter the command <code>help reference ospf hello-interval</code>.</p> <p>NOTE: In some cases, multiple Help topics are available for the same configuration statement. When an existing JUNOS statement has been modified for JUNOS Software, two <code>help</code> commands are available—one describing the original JUNOS statement and another describing the updates to that statement for JUNOS Software. To view the Help topic that describes the modifications made for JUNOS Software, enter the <code>help</code> command that contains the string <code>junos-es</code>. For example, to view Help for the <code>access profile <i>profile-name</i> authentication-order</code> statement, enter <code>help reference access authentication-order-junos-es</code>.</p>
<code>help topic <i>string</i></code>	<p>Displays usage guidelines for configuration statements.</p> <p>For example, to display usage guidelines for the OSPF hello interval, enter the command <code>help topic ospf hello-interval</code>.</p>

Configuring the CLI Environment

You can configure the CLI environment for your current login session. Your settings are not retained when you exit the CLI.

To display the current CLI settings, enter the `show cli` command:

```
user@host> show cli
CLI complete-on-space set to on CLI idle-timeout disabled CLI restart-on-upgrade
set to on CLI screen-length set to 49 CLI screen-width set to 132 CLI terminal
is 'vt100' CLI is operating in enhanced mode CLI working directory is
'/cf/var/home/remote'
```

To change the CLI environment, use the `set cli` operational mode command:

```

user@host> set cli ?
Possible completions:
complete-on-space  Set whether typing space completes current word
directory          Set working directory
idle-timeout       Set maximum idle time before login session ends
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

```

Table 66 on page 35 shows how you can change the CLI environment features.

Table 66: Configuring the CLI Environment

Environment Feature	CLI Command	Default Setting	Options
Command completion	set cli complete-on-space (on off)	on—Pressing Tab or Spacebar completes a command.	<ul style="list-style-type: none"> ■ Set off to allow only Tab for command completion. ■ Set on to re-enable Tab and Spacebar for command completion.
Your working directory	set cli directory <i>path</i> 8	/cf/var/home/remote	Replace <i>path</i> with the directory you want to enter when you log in to the device.
Minutes of idle time	set cli idle-time <i>minutes</i>	Your session never times out unless your login class specifies a timeout.	<ul style="list-style-type: none"> ■ To enable the timeout feature, replace <i>timeout</i> with a value between 1 and 100,000. ■ To disable the timeout feature, replace <i>timeout</i> with 0.
Your session prompt	set cli prompt <i>string</i>	<i>user@host ></i>	Replace <i>string</i> with the prompt you want. If the prompt contains spaces or special characters, enclose <i>string</i> in quotation marks (“ ”).
Restart-after-upgrade prompt	set cli restart-on-upgrade (on off)	CLI prompts you to restart the device after a software upgrade.	<ul style="list-style-type: none"> ■ Set off to disable the prompt for the session. ■ Set on to reenable the prompt.
Number of CLI output line displayed at once	set cli screen-length <i>length</i>	Variable (depends on terminal type).	<ul style="list-style-type: none"> ■ To change the number of lines displayed on the screen, replace <i>length</i> with a value between 1 and 100,000. ■ To disable the display of a set number of lines, replace <i>length</i> with 0. (This feature can be useful when you are issuing CLI commands from scripts.)
Number of CLI characters displayed on a line	set cli screen-width <i>width</i>	Variable (depends on terminal type).	To change the number of characters displayed on a line, replace <i>width</i> with a value between 0 and 100,000.

Table 66: Configuring the CLI Environment (*continued*)

Environment Feature	CLI Command	Default Setting	Options
Your terminal type.	set cli terminal <i>terminal-type</i>	unknown, or set by console.	Replace <i>terminal-type</i> with one of the following values: <ul style="list-style-type: none">■ ansi■ vt100■ small-xterm■ xterm

Chapter 6

Configuring Secure Web Access

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses 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 Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

You can use J-Web Quick Configuration, the J-Web configuration editor, or the CLI configuration editor to configure secure Web access.

For more information about the J-Web interface, see the *J-Web Interface User Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Secure Web Access Terms on page 37
- Secure Web Access Overview on page 38
- Before You Begin on page 38
- Configuring Management Access on page 39
- Configuring Secure Web Access with a Configuration Editor on page 42
- Verifying Secure Web Access on page 43

Secure Web Access Terms

Before configuring secure Web access, become familiar with the terms defined in Table 67 on page 37.

Table 67: Secure Web Access Terms

Term	Definition
certificate authority (CA)	Third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The CA guarantees the identity of the individual or device that presents the digital certificate.

Table 67: Secure Web Access Terms *(continued)*

Term	Definition
Hypertext Transfer Protocol (HTTP)	Protocol used to publish and receive information on the Web, such as text and graphics files.
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	Protocol similar to HTTP with an added encryption layer that encrypts and decrypts user page requests and pages that are returned by a Web server. HTTPS is used for secure communication, such as payment transactions.
Privacy-Enhanced Mail (PEM)	Technique for securely exchanging electronic mail over a public medium. PEM is based upon public key infrastructure (PKI) standards like X.509 certificates. SSL certificates are partly based on PEM and end in the suffix <code>.pem</code> .
RSA	Public key cipher that can be used for encrypting messages and making digital signatures. RSA uses a well-known encryption and authentication algorithm that is a part of popular Web browsers.
Secure Sockets Layer (SSL)	Protocol that encrypts security information before transmitting data across a network. SSL requires two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message—and an authentication certificate. Most popular Web browsers support SSL.
SSL certificate	Secure electronic identifier conforming to the X.509 standard, definitively identifying an individual, system, company, or organization. In addition to identification data, the digital certificate contains a serial number, a copy of the certificate holder's public key, the identity and digital signature of the issuing certificate authority (CA), and an expiration date.

Secure Web Access Overview

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 are not able to access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

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.

Before You Begin

Before you begin initial configuration, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Obtain an SSL certificate from a trusted signing authority. See “Generating SSL Certificates” on page 39.

Generating SSL Certificates

To enable secure Web access, you must first generate a digital SSL certificate, and then enable HTTPS access on the device.

To generate an SSL certificate:

1. Enter the following **openssl** command in your Secure Shell command-line interface. The **openssl** command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

```
% openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
```

Replace *filename* with the name of a file in which you want the SSL certificate to be written—for example, **new.pem**.

2. When prompted, type the appropriate information in the identification form. For example, type **US** for the country name.
3. Display the contents of the file **new.pem**.

```
cat new.pem
```

Copy the contents of this file for installing the SSL certificate.

You can use either J-Web Quick Configuration or a configuration editor to install the SSL certificate and enable HTTPS.

Configuring Management Access

To configure device access options, such as HTTPS and certificates, select **Configure > System Properties > Management Access** in the J-Web user interface.

This section includes the following instructions:

- Configuring Device Addresses on page 40
- Enabling Access Services on page 40
- Adding, Editing, and Deleting Certificates on the Device on page 41

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.

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 JUNOScript 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 JUNOScript XML scripting API, select **Enable JUNOScript over clear text** or **Enable JUNOScript over SSL**. If you enable JUNOScript over SSL, select the certificate you want to use for encryption from the **JUNOScript 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 JUNOScript access—A JUNOScript client such as JUNOScope is required. For information about how to log in to JUNOScope, see the *JUNOScope Software User Guide*.

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 JUNOScript sessions. (For information about how to generate an SSL certificate to upload to the device, see “Generating SSL Certificates” on page 39.)

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.

Configuring Secure Web Access with a Configuration Editor

You can manage your Juniper Networks device using a secure Web connection by enabling HTTPS.

To enable HTTPS on your device:

1. In either the J-Web or CLI configuration editor, navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 68 on page 42.
3. If you are finished configuring the device, commit the configuration.
4. To check the configuration, see “Verifying Secure Web Access” on page 43.

Table 68: Configuring a Secure Web Access

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Security level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Security, click Configure or Edit. 	From the [edit] hierarchy level, enter edit security
Import the SSL certificate that you have generated—for example, new . For information about generating SSL certificates, see “Generating SSL Certificates” on page 39.	<ol style="list-style-type: none"> 1. Next to Certificates, click Configure. 2. Next to Local, click Add new entry. 3. In the Name box, type a name for the certificate to be imported—for example, new. 4. In the Certificate box, paste the generated SSL certificate and private key. 5. Click OK. 	Enter set certificates local new load-key-filepath Replace <i>path</i> with a path or URL to the file containing an SSL certificate and private key in PEM format—for example, <code>/var/tmp/new.pem</code>
Enable HTTPS access and specify the SSL certificate to be used for authentication.	<ol style="list-style-type: none"> 1. On the main Configuration page next to System, click Configure or Edit. 2. Select the Services check box and click Edit next to it. 	From the [edit system] hierarchy level, enter set services web-management https local-certificate new port 8443
Specify the port on which HTTPS access is to be enabled—for example, TCP port 8443. NOTE: You can enable HTTPS access on specified interfaces also. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.	<ol style="list-style-type: none"> 3. Next to Web management, click Edit. 4. Select the Https check box and click Edit next to it. 5. In the Local certificate box, type the name of the certificate—for example, new. 6. In the Port box, type 8443. 7. Click OK. 	

Verifying Secure Web Access

To verify that the device has the secure access settings you configured, perform the following tasks:

- Displaying an SSL Certificate Configuration on page 43
- Displaying a Secure Access Configuration on page 43

Displaying an SSL Certificate Configuration

Purpose Display the SSL certificate configuration.

Action From the J-Web interface, select **CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the **show security** command.

The following sample output displays an SSL certificate generated with instructions in “Generating SSL Certificates” on page 39:

```
[edit]
user@R0# show security
certificates {
  local {
    new {
      "—BEGIN RSA PRIVATE KEY—\nMIICXQIBAAKBgQC/C5UI4frNqbi
      qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hA0rCnb0YO+SY
      Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBlw7/MJ+OpA
      ... KYiFf4CbBBbjIMQJOHFudW6ISVBslONkzX+FT\ni95ddka6ilRnArEb4VFCRh+
      e1QBdp1UjziYf7NuzDx4Z\n —END RSA PRIVATE KEY—\n—BEGIN
      CERTIFICATE— \nMIIDjDCCAyVwAwIBAgIBADANBgkqhkiG9w0BAQQ ...
      FADCBkTElMAkGA1UEBhMCdXMx\nCzAJBgNVBAGTAzAmNhMRlwEAYDVQQHEwldW5ue
      HB1YnMxDTALBgNVBAMTBGpucHlxJDAiBgkqhkiG9w0BCQEWFW5iaGFyZ2F2YUB
      fLUYAnBYmsYWOH\n —END CERTIFICATE—\n"; ## SECRET-DATA
    }
  }
}
```

Meaning The output shows the intended secure access configuration.

Related Topics For more information about the format of a configuration file, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Displaying a Secure Access Configuration

Purpose Verify the secure access configuration.

Action From the J-Web interface, select **CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the **show system services** command.

The following sample output displays the sample values for secure Web access as configured in Table 68 on page 42:

```
[edit]
```

```
user@R0# show system services  
web-management {  
  http;  
  https {  
    port 8443;  
    local-certificate new;  
  }  
}
```

Meaning The output shows the intended secure access configuration.

Related Topics For more information about the format of a configuration file, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Chapter 7

Managing Administrator Authentication

You can use either J-Web Quick Configuration or a configuration editor to manage system functions, including RADIUS and TACACS+ servers, and user login accounts.



NOTE: In this chapter, user authentication refers to administrator authentication. For information about firewall user authentication, see the *JUNOS Software Security Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

For more information about system management, see the *JUNOS System Basics Configuration Guide*.

This chapter contains the following topics.

- User Authentication Terms on page 45
- User Authentication Overview on page 46
- Before You Begin on page 50
- Managing User Authentication on page 50
- Managing User Authentication with a Configuration Editor on page 52
- Securing the Console Port on page 61
- Accessing Remote Devices with the CLI on page 62
- Configuring Password Retry Limits for Telnet and SSH Access on page 64
- Reverse Telnet on page 65

User Authentication Terms

Before performing system management tasks, become familiar with the terms defined in Table 69 on page 46.

Table 69: System Management Terms

Term	Definition
Remote Authentication Dial-In User Service (RADIUS)	Authentication method for validating users who attempt to access one or more services routers by means of Telnet. RADIUS is a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS.
Terminal Access Controller Access Control System Plus (TACACS+)	Authentication method for validating users who attempt to access one or more services routers by means of Telnet.

User Authentication Overview

This section contains the following topics:

- User Authentication on page 46
- User Accounts on page 46
- Login Classes on page 47
- Template Accounts on page 50

User Authentication

JUNOS Software 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

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 the device will try first.

User Accounts

User accounts provide one way for users to access the services router. Users can access the device without accounts if you configured RADIUS or TACACS+ servers, as described in “Managing User Authentication” on page 50 and “Managing User Authentication with a Configuration Editor” on page 52. 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 information about configuring the password for the user **root**, see the *JUNOS Software Administration Guide*. 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 must be in the range 100 through 64000 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 default classes listed in Table 70 on page 47.
- 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 Software 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.

Login Classes

All users who log into the services router 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. For more information, see “Permission Bits” on page 47.
- Commands and statements that users can and cannot specify. For more information, see “Denying or Allowing Individual Commands” on page 49.
- How long a login session can be idle before it times out and the user is logged off.

The software contains a few predefined login classes, which are listed in Table 70 on page 47. The predefined login classes cannot be modified.

Table 70: Predefined Login Classes

Login Class	Permission Bits Set
operator	clear, network, reset, trace, view
read-only	view
super-user and superuser	all
unauthorized	None

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 71 on page 48).

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 71: Permission Bits for Login Classes

Permission Bit	Access
admin	Can view user account information in configuration mode and with the <code>show configuration</code> command.
admin-control	Can view user accounts and configure them (at the <code>[edit system login]</code> hierarchy level).
access	Can view the access configuration in configuration mode and with the <code>show configuration</code> operational mode command.
access-control	Can view and configure access information (at the <code>[edit access]</code> hierarchy level).
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the <code>clear</code> commands).
configure	Can enter configuration mode (using the <code>configure</code> command) and commit configurations (using the <code>commit</code> command).
control	Can perform all control-level operations (all operations configured with the <code>-control</code> permission bits).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the <code>[edit firewall]</code> hierarchy level).
floppy	Can read from and write to the removable media.
interface	Can view the interface configuration in configuration mode and with the <code>show configuration</code> operational mode command.
interface-control	Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the <code>[edit]</code> hierarchy).
maintenance	Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the <code>su root</code> command), and can halt and reboot the device (using the <code>request system</code> commands).
network	Can access the network by entering the <code>ping</code> , <code>ssh</code> , <code>telnet</code> , and <code>traceroute</code> commands.

Table 71: Permission Bits for Login Classes *(continued)*

Permission Bit	Access
reset	Can restart software processes using the restart command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level).
rollback	Can use the rollback command to return to a previously committed configuration other than the most recently committed one.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.
security-control	Can view and configure security information (at the [edit security] hierarchy level).
shell	Can start a local shell on the device by entering the start shell command.
snmp	Can view SNMP configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the [edit system] hierarchy level).
trace	Can view trace file settings in configuration and operational modes.
trace-control	Can view trace file settings and configure trace file properties.
view	Can use various commands to display current systemwide, 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.

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 services router and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, JUNOS Software 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.

For more information, see “Setting Up Template Accounts” on page 59.

Before You Begin

Before you perform any system management tasks, you must perform the initial device configuration described in the Getting Started Guide for your device.

Managing User Authentication

This section contains the following topics:

- Adding a RADIUS Server or TACACS Server for Authentication on page 50
- Configuring System Authentication on page 51
- Adding New Users on page 51

Adding a RADIUS Server or TACACS Server for Authentication

You can use the User Management page to configure a RADIUS server or TACACS server for system authentication.

To configure a RADIUS server or TACACS server:

1. In the J-Web 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 or TACACS section, click **Add**. Either the Add Radius Server dialog box or Add TACACS Server dialog box appears.
5. In the **IP Address** field, enter the server's 32-bit IP address.
6. In the **Password** and **Confirm Password** fields, enter the secret password for the server and verify your entry.
7. In the **Server Port** field, enter the appropriate port.

8. In the **Source Address** field, enter the source IP address of the server.
9. In the **Retry Attempts** field, specify the number of times that the server should try to verify the user's credentials.
10. In the **Time Out** field, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK**.

Configuring System Authentication

You can use the User Management page to 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.

To configure system authentication:

1. In the J-Web 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 and down arrows to specify the order in which the device should execute the authentication methods.
6. Click **OK**.

Adding New Users

You can use the User Management page to 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.

To configure users:

1. In the J-Web 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** field, enter a unique name for the user.

Do not include spaces, colons, or commas in the username.

6. In the **User ID** field, enter a unique ID for the user.
7. In the **Full Name** field, enter 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** fields, enter a login password for the user and verify your entry. The login password must meet the following criteria:
 - The password must be at least 6 characters long.
 - You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.
 - The password must contain at least one change of case or character class.
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. For more information, see "Login Classes" on page 47.

10. Click **OK** in the Add User dialog box and Edit User Management dialog box.

Managing User Authentication with a Configuration Editor

This section contains the following topics:

- Setting Up RADIUS Authentication on page 52
- Setting Up TACACS+ Authentication on page 54
- Configuring Authentication Order on page 55
- Controlling User Access on page 56
- Setting Up Template Accounts on page 59

Setting Up RADIUS Authentication

To use RADIUS authentication, you must configure at least one RADIUS server.

The procedure provided in this section identifies the RADIUS server, specifies the secret (password) of the RADIUS server, and sets the source address of the services

router's RADIUS requests to the loopback address of the device. The procedure uses the following sample values:

- The RADIUS server's IP address is **172.16.98.1**.
- The RADIUS server's secret is **Radiussecret1**.
- The loopback address of the device is **10.0.0.1**.

To configure RADIUS authentication:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 72 on page 53.
3. If you are finished configuring the network, commit the configuration.

To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order.

4. Go on to one of the following procedures:
 - To specify a system authentication order, see “Configuring Authentication Order” on page 55.
 - To configure a remote user template account, see “Creating a Remote Template Account” on page 59.
 - To configure local user template accounts, see “Creating a Local Template Account” on page 60.

Table 72: Setting Up RADIUS Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system
Add a new RADIUS server	<ol style="list-style-type: none"> 1. In the Radius server box, click Add new entry. 2. In the Address box, type the IP address of the RADIUS server: 172.16.98.1 	Set the IP address of the RADIUS server: set radius-server address 172.16.98.1
Specify the shared secret (password) of the RADIUS server. The secret is stored as an encrypted value in the configuration database.	In the Secret box, type the shared secret of the RADIUS server: Radiussecret1	Set the shared secret of the RADIUS server: set radius-server 172.16.98.1 secret Radiussecret1

Table 72: Setting Up RADIUS Authentication *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
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.	In the Source address box, type the loopback address of the device: 10.0.0.1	Set the device's loopback address as the source address: set radius-server 172.16.98.1 source-address 10.0.0.1

Setting Up TACACS+ Authentication

To use TACACS+ authentication, you must configure at least one TACACS+ server.

The procedure provided in this section identifies the TACACS+ server, specifies the secret (password) of the TACACS+ server, and sets the source address of the services router's TACACS+ requests to the loopback address of the device. This procedure uses the following sample values:

- The TACACS+ server's IP address is 172.16.98.24.
- The TACACS+ server's secret is Tacacssecret1.
- The loopback address of the device is 10.0.0.1.

To configure TACACS+ authentication:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 73 on page 55.
3. If you are finished configuring the network, commit the configuration.

To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order.

4. Go on to one of the following procedures:
 - To specify a system authentication order, see “Configuring Authentication Order” on page 55.
 - To configure a remote user template account, see “Creating a Remote Template Account” on page 59.
 - To configure local user template accounts, see “Creating a Local Template Account” on page 60.

Table 73: Setting Up TACACS+ Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system
Add a new TACACS+ server	<ol style="list-style-type: none"> 1. In the Tacplus server box, click Add new entry. 2. In the Address box, type the IP address of the TACACS+ server: 172.16.98.24 	Set the IP address of the TACACS+ server: set tacplus-server address 172.16.98.24
Specify the shared secret (password) of the TACACS+ server. The secret is stored as an encrypted value in the configuration database.	<p>In the Secret box, type the shared secret of the TACACS+ server:</p> <p>Tacacssecret1</p>	Set the shared secret of the TACACS+ server: set tacplus-server 172.16.98.24 secret Tacacssecret1
Specify the source address to be included in the TACACS+ server requests by the device. In most cases, you can use the loopback address of the device.	<p>In the Source address box, type the loopback address of the device:</p> <p>10.0.0.1</p>	Set the device's loopback address as the source address: set tacplus-server 172.16.98.24 source-address 10.0.0.1

Configuring Authentication Order

The procedure provided in this section configures the services router to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

To configure authentication order:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 74 on page 56.
3. If you are finished configuring the network, commit the configuration.

To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts.

4. Go on to one of the following procedures:
 - To configure a RADIUS server, see “Setting Up RADIUS Authentication” on page 52.
 - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 54.

- To configure a remote user template account, see “Creating a Remote Template Account” on page 59.
- To configure local user template accounts, see “Creating a Local Template Account” on page 60.

Table 74: Configuring Authentication Order

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system
Add RADIUS authentication to the authentication order.	<ol style="list-style-type: none"> 1. In the Authentication order box, click Add new entry. 2. In the list, select radius. 3. Click OK. 	Insert the radius statement in the authentication order: insert system authentication-order radius after password
Add TACACS+ authentication to the authentication order.	<ol style="list-style-type: none"> 1. In the Authentication Order box, click Add new entry. 2. In the list, select tacplus. 3. Click OK. 	Insert the tacplus statement in the authentication order: insert system authentication-order tacplus after radius

Controlling User Access

This section contains the following topics:

- Defining Login Classes on page 56
- Creating User Accounts on page 58

Defining Login Classes

You can define any number of login classes. You then apply one login class to an individual user account, as described in “Creating User Accounts” on page 58 and “Setting Up Template Accounts” on page 59.

The procedure provided in this section creates a sample login class named **operator-and-boot** with the following privileges:

- The **operator-and-boot** login class can reboot the services router using the **request system reboot** command.
- The **operator-and-boot** login class can also use commands defined in the **clear**, **network**, **reset**, **trace**, and **view** permission bits. For more information, see “Permission Bits” on page 47.

To define login classes:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 75 on page 57.
3. If you are finished configuring the network, commit the configuration.
4. Go on to one of the following procedures:
 - To create user accounts, see “Creating User Accounts” on page 58.
 - To create shared user accounts, see “Setting Up Template Accounts” on page 59.

Table 75: Defining Login Classes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System Login level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Login, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit system login</p>
Create a login class named operator-and-boot with the ability to reboot the device.	<ol style="list-style-type: none"> 1. Next to Class, click Add new entry. 2. Type the name of the login class: <p>operator-and-boot</p> 3. In the Allow commands box, type the request system reboot command enclosed in quotation marks: <p>“request system reboot”</p> 4. Click OK. 	<p>Set the name of the login class and the ability to use the request system reboot command:</p> <p>set class operator-and-boot allow-commands “request system reboot”</p>

Table 75: Defining Login Classes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Give the <code>operator-and-boot</code> login class operator privileges.	<ol style="list-style-type: none"> Next to Permissions, click Add new entry. In the Value list, select clear. Click OK. Next to Permissions, click Add new entry. In the Value list, select network. Click OK. Next to Permissions, click Add new entry. In the Value list, select reset. Click OK. Next to Permissions, click Add new entry. In the Value list, select trace. Click OK. Next to Permissions, click Add new entry. In the Value list, select view. Click OK. 	<p>Set the permission bits for the <code>operator-and-boot</code> login class:</p> <pre>set class operator-and-boot permissions [clear network reset trace view]</pre>

Creating User Accounts

User accounts provide one way for users to access the services router. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers, as described in “Setting Up RADIUS Authentication” on page 52 and “Setting Up TACACS+ Authentication” on page 54.)

The procedure provided in this section creates a sample user named `cmartin` with the following characteristics:

- The user `cmartin` belongs to the `superuser` login class.
- The user `cmartin` uses an encrypted password, `$1$14c5.$sBopasdFFdssdfFFdsdfsO`.

To create user accounts:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- Perform the configuration tasks described in Table 76 on page 59.
- If you are finished configuring the network, commit the configuration.

Table 76: Creating User Accounts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System Login level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Login, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system login
Create a user named cmartin who belongs to the superuser login class.	<ol style="list-style-type: none"> 1. Next to User, click Add new entry. 2. In the User name box, type cmartin. 3. In the Class box, type superuser. 4. Click OK. 	Set the username and the login class for the user: set user cmartin class superuser
Define the encrypted password for cmartin .	<ol style="list-style-type: none"> 1. Next to Authentication, click Configure. 2. In the Encrypted password box, type \$1\$14c5.\$sBopasdFFdssdffFFdsdfs0 3. Click OK. 	Set the encrypted password for cmartin . set user cmartin authentication encrypted-password \$1\$14c5.\$sBopasdFFdssdffFFdsdfs0

Setting Up Template Accounts

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.

This section contains the following topics:

- Creating a Remote Template Account on page 59
- Creating a Local Template Account on page 60

Creating a Remote Template Account

You can create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

By default, JUNOS Software uses the **remote** template account when

- The authenticated user does not exist locally on the services router.
- 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.

The procedure provided in this section creates a sample user named **remote** that belongs to the **operator** login class.

To create a remote template account:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 77 on page 60.
3. If you are finished configuring the network, commit the configuration.

To completely set up RADIUS or TACACS + authentication, you must configure at least one RADIUS or TACACS + server and specify a system authentication order.

4. Go on to one of the following procedures:
 - To configure a RADIUS server, see “Setting Up RADIUS Authentication” on page 52.
 - To configure a TACACS + server, see “Setting Up TACACS + Authentication” on page 54.
 - To specify a system authentication order, see “Configuring Authentication Order” on page 55.

Table 77: Creating a Remote Template Account

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System Login level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Login, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system login
Create a user named remote who belongs to the operator login class.	<ol style="list-style-type: none"> 1. Next to User, click Add new entry. 2. In the User name box, type remote. 3. In the Class box, type operator. 4. Click OK. 	Set the username and the login class for the user: set user remote class operator

Creating a Local Template Account

You can create a local template that is applied to users authenticated by RADIUS or TACACS + that are assigned to the local template account. 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.

The procedure provided in this section creates a sample user named **admin** that belongs to the **superuser** login class.

To create a local template account:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 78 on page 61.
3. If you are finished configuring the network, commit the configuration.

To completely set up RADIUS or TACACS + authentication, you must configure at least one RADIUS or TACACS + server and specify a system authentication order

4. Go on to one of the following procedures:
 - To configure a RADIUS server, see “Setting Up RADIUS Authentication” on page 52.
 - To configure a TACACS + server, see “Setting Up TACACS + Authentication” on page 54.
 - To configure a system authentication order, see “Configuring Authentication Order” on page 55.

Table 78: Creating a Local Template Account

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System Login level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Login, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system login
Create a user named admin who belongs to the superuser login class.	<ol style="list-style-type: none"> 1. Next to User, click Add new entry. 2. In the User name box, type admin. 3. In the Class box, type superuser. 4. Click OK. 	Set the username and the login class for the user: set user admin class superuser

Securing the Console Port

You can use the console port on the device to connect to the Routing Engine 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 do the following:

- Log out the console session when you unplug the serial cable connected to the console port.
- Disable root login connections to 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).

To secure the console port:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 79 on page 62.
3. If you are finished configuring the network, commit the configuration.

Table 79: Securing the Console Port

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Console level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Ports, click Configure or Edit. 4. Next to Console, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit system ports console</p>
Secure the console port.	<ol style="list-style-type: none"> 1. Select one of the following check boxes: <ul style="list-style-type: none"> ■ Disable—Console port is disabled. ■ Insecure—Root login connections to the console are disabled. ■ Log out on disconnect—Logs out the console session when the serial cable connected to the console port is unplugged. 2. Click OK. 	<p>Do one of the following:</p> <ul style="list-style-type: none"> ■ To disable the console port, enter set disable ■ To disable root login connections to the console, enter set insecure ■ To log out the console session when the serial cable connected to the console port is unplugged, enter set log-out-on-disconnect

Accessing Remote Devices with the CLI

This section contains the following topics:

- Using the telnet Command on page 62
- Using the ssh Command on page 63

Using 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>
```

To escape from the Telnet session to the Telnet command prompt, press Ctrl-]. To exit from the Telnet session and return to the CLI command prompt, enter **quit**.

Table 80 on page 63 describes the **telnet** command options. For more information, see the *JUNOS System Basics and Services Command Reference*.

Table 80: CLI telnet Command Options

Option	Description
8bit	Use an 8-bit data path.
bypass-routing	Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open a Telnet session to the specified hostname or IP address.
inet	Force the Telnet session to an IPv4 destination.
interface <i>source-interface</i>	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
no-resolve	Suppress the display of symbolic names.
port <i>port</i>	Specify the port number or service name on the host.
routing-instance <i>routing-instance-name</i>	Use the specified routing instance for the Telnet session.
source <i>address</i>	Use the specified source address for the Telnet session.

Using 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>
```

Table 81 on page 63 describes the **ssh** command options. For more information, see the *JUNOS System Basics and Services Command Reference*.

Table 81: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.

Table 81: CLI ssh Command Options (*continued*)

Option	Description
<code>interface <i>source-interface</i></code>	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
<code>routing-instance <i>routing-instance-name</i></code>	Use the specified routing instance for the SSH connection.
<code>source <i>address</i></code>	Use the specified source address for the SSH connection.
<code>v1</code>	Force SSH to use version 1 for the connection.
<code>v2</code>	Force SSH to use version 2 for the connection.

Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the services router 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 services router 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 services router to take the following actions for Telnet and SSH sessions:

- Allow a maximum of 4 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. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 82 on page 65.
3. If you are finished configuring the network, commit the configuration.

Table 82: Configuring Password Retry Limits for Telnet and SSH Access

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Retry options level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Edit. 3. Next to Login, click Configure or Edit. 4. Next to Retry options, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit system login retry-options</p>
Configure password retry limits for Telnet and SSH access. <ul style="list-style-type: none"> ■ Tries—Maximum number of consecutive password retries before a SSH or Telnet sessions is disconnected. The default number is 10, but you can set a number between 1 and 10. ■ Backoff threshold—Threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is 2, but you can set a number between 1 and 3. ■ Backoff factor—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 set a delay between 5 and 10 seconds. ■ Minimum time—Minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is 20 seconds, but you can set a time between 20 and 60 seconds. 	<ol style="list-style-type: none"> 1. In the Tries before disconnect box, type 4. 2. In the Backoff threshold box, type 2. 3. In the Backoff factor box, type 5. 4. In the Minimum time box, type 40. 5. Click OK. 	<ol style="list-style-type: none"> 1. Enter set tries-before-disconnect 4 2. Enter set backoff-threshold 2 3. Enter set backoff-factor 5 4. Enter set minimum-time 40

Reverse Telnet

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 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.

- Reverse Telnet Overview on page 65
- Configuring Reverse Telnet and Reverse SSH on page 66

Reverse Telnet Overview

In order to use reverse Telnet, you must have the following:

- A device with an auxiliary port running the appropriate version of JUNOS Software
- A device with a console port for remote management if network connectivity fails and you want to use console access

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: If you want to enable reverse SSH, you must explicitly enter the command to do so. By default, when you enable reverse Telnet, the connection is not encrypted.

Reverse Telnet Restrictions

The following restrictions exist when you are attempting 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.

Configuring Reverse Telnet and Reverse SSH

This topic contains the following section:

- CLI Configuration on page 66

CLI Configuration

1. To enable reverse Telnet, enter the following:

```
user@host# set system services reverse telnet
```

2. You can specify the port for reverse Telnet. If you do not specify a port, 2900 is the default port that is used.

```
user@host# set system services reverse telnet port 5000
```

3. You can enable reverse SSH to encrypt the connection between the device and the client.

```
user@host# set system services reverse ssh
```

4. You can specify the port for reverse SSH. If you do not specify a port, 2901 is the default port that is used.

```
user@host# set system services reverse ssh port 6000
```

Chapter 8

Setting Up USB Modems for Remote Management

J Series Services Routers 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.



NOTE: We recommend using a Multi-Tech MultiModem MT5634ZBA-USB-V92 USB modem with J Series Service Routers.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics:

- USB Modem Terms on page 67
- USB Modem Overview on page 68
- Before You Begin on page 71
- Connecting the USB Modem to the USB Port on page 71
- Configuring USB Modem Interfaces with a Configuration Editor on page 71
- Connecting to the Device from the User End on page 77
- Administering USB Modems on page 78
- Verifying the USB Modem Configuration on page 80

USB Modem Terms

Before configuring USB modems and their supporting dialer interfaces, become familiar with the terms defined in Table 83 on page 68.

Table 83: USB Modem Terminology

Term	Definition
caller ID	Telephone number of the caller on the remote end of a USB modem connection, used to dial in and also to identify the caller. Multiple caller IDs can be configured on a dialer interface. During dial-in, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.
dialer interface (dl)	Logical interface for configuring dialing properties for a USB modem connection.
dial-in	Feature that enables the device to receive calls from the remote end of a USB modem connection. The remote end of the USB modem call might be a service provider, a corporate central location, or a customer premises equipment (CPE) branch office. All incoming calls can be verified against caller IDs configured on the device's dialer interface.
Microcom Networking Protocol (MNP)	Protocol that provides error correction and data compression for asynchronous modem transmission.

USB Modem Overview

A USB modem connects to a services router 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.

- USB Modem Interfaces on page 68
- How the Device Initializes USB Modems on page 69
- USB Modem Connection and Configuration Overview on page 70

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity: a physical interface and a logical interface called the dialer interface:

- The USB modem physical interface uses the naming convention `umd0`. The services router creates this interface when a USB modem is connected to the USB port.
- The dialer interface, `dln`, is a logical interface for configuring dialing properties for USB modem connections.

See the interface naming conventions in the *JUNOS Software Interfaces and Routing Configuration Guide*.

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.
- If you are using the same dialer interface for ISDN connections and USB modem connections, the dialer interface cannot be configured simultaneously in the following modes:
 - As a backup interface and a dialer filter
 - As a backup interface and dialer watch interface
 - As a dialer watch interface and a dialer filter
 - As a backup interface for more than one primary interface

How the Device Initializes USB Modems

When you connect the USB modem to the USB port on the services router, the device applies the modem AT commands configured in the `init-command-string` command to the initialization commands on the modem. For more information about configuring modem commands for the `init-command-string` command, see “Modifying USB Modem Initialization Commands” on page 79.

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 84 on page 69 describes the commands. For more information about these commands, see the documentation for your modem.

Table 84: Default Modem Initialization Commands

Modem Command	Description
AT	Attention. Informs the modem that a command follows.
S7=45	Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
S0=0	Disables the auto answer feature, whereby the modem automatically answers calls.
V1	Displays result codes as words.
&C1	Disables reset of the modem when it loses the carrier signal.
E0	Disables the display on the local terminal of commands issued to the modem from the local terminal.
Q0	Enables the display of result codes.
&Q8	Enables Microcom Networking Protocol (MNP) error control mode.

Table 84: Default Modem Initialization Commands (*continued*)

Modem Command	Description
%CO	Disables data compression.

When the services router 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 services router 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.

USB Modem Connection and Configuration Overview

To use USB modems to remotely manage a services router, you perform the tasks listed in Table 85 on page 70. For instructions, see the cross-references in the table.

Table 85: USB Modem Connection and Configuration Overview

Task	Instructions
Perform prerequisite tasks.	"Before You Begin" on page 71
On the Services Router	
1. Connect a modem to the device.	"Connecting the USB Modem to the USB Port" on page 71
2. Configure the modem interfaces on the device.	"Configuring USB Modem Interfaces with a Configuration Editor" on page 71
3. Verify the modem configuration on the device.	"Verifying the USB Modem Configuration" on page 80
4. Perform administrative tasks as necessary.	<ul style="list-style-type: none"> ■ Modifying USB Modem Initialization Commands on page 79 ■ Resetting USB Modems on page 80
At the User End	
1. Configure the modem at your remote location.	"Configuring a Dial-Up Modem Connection at the User End" on page 77
2. Dial in to the device.	"Connecting to the Device from the User End" on page 78

Before You Begin

Before you configure USB modems, you need to perform the following tasks:

- Install device hardware. For more information, see the Getting Started Guide for your device.
- Establish basic connectivity. For more information, see the Getting Started Guide for your device.
- Order a Multi-Tech MultiModem MT5634ZBA-USB-V92 USB modem from Multi-Tech Systems (<http://www.multitech.com/>).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the services router.
- Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Connecting the USB Modem to the USB Port



NOTE: J4350 and J6350 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.

To connect the USB modem to the USB port on the device:

1. Plug the modem into the USB port.
2. Connect the modem to your telephone network.

Configuring USB Modem Interfaces with a Configuration Editor

To configure USB modem interfaces, perform the following tasks marked *(Required)*. Perform other tasks if needed on your network.

- Configuring a USB Modem Interface (Required) on page 71
- Configuring a Dialer Interface (Required) on page 73
- Configuring Dial-In (Required) on page 74
- Configuring CHAP on Dialer Interfaces (Optional) on page 75

Configuring a USB Modem Interface (Required)

To configure a USB modem interface for the device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 86 on page 72.
3. Go on to “Configuring a Dialer Interface (Required)” on page 73.

Table 86: Configuring a USB Modem Interface

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Interfaces, click Configure or Edit. 	From the [edit] hierarchy level, enter edit interfaces umd0
Create the new interface umd0 .	<ol style="list-style-type: none"> 1. Next to Interface, click Add new entry. 2. In the Interface name box, type the name of the new interface, umd0. 3. Click OK. 	
Configure dialer options. ■ Name the dialer pool configured on the dialer interface you want to use for USB modem connectivity—for example, usb-modem-dialer-pool . For more information, see “Configuring a Dialer Interface (Required)” on page 73. ■ Set the dialer pool priority—for example, 25 . Dialer pool priority has a range from 1 to 255 , with 1 designating lowest-priority interfaces and 255 designating the highest-priority interfaces.	<ol style="list-style-type: none"> 1. In the Encapsulation column, next to the new interface, click Edit. 2. Next to Dialer options, select Yes, and then click Configure. 3. Next to Pool, click Add new entry. 4. In the Pool identifier box, type usb-modem-dialer-pool. 5. In the Priority box, type 25. 6. Click OK until you return to the Interface page. 	Enter set dialer-options pool usb-modem-dialer-pool priority 25
The S0=0 command in the default modem initialization sequence AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0 , disables the modem from automatically answering calls. Configure the modem to automatically answer calls after a specified number of rings. For more information about modem initialization commands, see “How the Device Initializes USB Modems” on page 69 and “Modifying USB Modem Initialization Commands” on page 79.	<ol style="list-style-type: none"> 1. Next to Modem options, click Configure. 2. In the Init command string box, type ATS0=2 to configure the modem to automatically answer after two rings. 3. Click OK. 	Enter set modem-options init-command-string "ATS0=2 \n"

Configuring a Dialer Interface (Required)

The dialer interface (dl) is a logical interface configured to establish USB modem connectivity. You can configure multiple dialer interfaces for different functions on the device.

To configure a logical dialer interface for the device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 87 on page 73.
3. Go on to “Configuring Dial-In (Required)” on page 74.

Table 87: Adding a Dialer Interface to a Device

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Interfaces, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit interfaces</p>
<p>Create the new interface—for example, dl0.</p> <p>Adding a description can differentiate between different dialer interfaces—for example, USB-modem-remote-management.</p>	<ol style="list-style-type: none"> 1. Next to Interface, click Add new entry. 2. In the Interface name box, type dl0. 3. In the Description box, type USB-modem-remote-management. 4. Click OK. 	<p>Create and name the interface:</p> <ol style="list-style-type: none"> 1. edit dl0 2. set description USB-modem-remote-management
<p>Configure Point-to-Point Protocol (PPP) encapsulation.</p> <p>NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.</p>	<ol style="list-style-type: none"> 1. In the Encapsulation column, next to the new interface, click Edit. 2. From the Encapsulation list, select PPP. 	<p>Enter</p> <p>set encapsulation ppp</p>
<p>Create the logical unit 0.</p> <p>NOTE: The logical unit number must be 0.</p>	<ol style="list-style-type: none"> 1. Next to Unit, click Add new entry. 2. In the Interface unit number box, type 0. 3. Next to Dialer options, select Yes, and then click Configure. 	<p>Enter</p> <p>set unit 0</p>

Table 87: Adding a Dialer Interface to a Device (*continued*)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the name of the dialer pool to use for USB modem connectivity—for example, <code>usb-modem-dialer-pool</code> .	<ol style="list-style-type: none"> 1. In the Pool box, type <code>usb-modem-dialer-pool</code>. 2. Click OK. 	<ol style="list-style-type: none"> 1. Enter edit unit 0 2. Enter set dialer-options pool usb-modem-dialer-pool
Configure source and destination IP addresses for the dialer interface—for example, <code>172.20.10.2</code> and <code>172.20.10.1</code> . 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.	<ol style="list-style-type: none"> 1. Select Inet under Family, and click Configure. 2. Next to Address, click Add new entry. 3. In the Source box, type <code>172.20.10.2</code>. 4. In the Destination box, type <code>172.20.10.1</code>. 5. Click OK. 	<p>Enter</p> <p>set family inet address 172.20.10.2 destination 172.20.10.1</p>

Configuring Dial-In (Required)

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.

To configure a dialer interface for dial-in:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 88 on page 75.

3. If you are finished configuring the device, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the USB Modem Configuration” on page 80.

Table 88: Configuring the Dialer Interface for Dial-In

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy, and select a dialer interface—for example, d10 .	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Interfaces, click Edit. 3. Next to d10, click Edit. 	From the [edit] hierarchy level, enter edit interfaces d10
<p>On logical interface 0 configure the incoming map options for the dialer interface.</p> <ul style="list-style-type: none"> ■ 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. 	<ol style="list-style-type: none"> 1. In the Unit section, for logical unit number 0, click Dialer options under Nested Configuration. 2. Next to Incoming map, click Configure. 3. From the Caller type menu, select Caller. 4. Next to Caller, click Add new entry. 5. In the Caller id box, type 4085550115. 6. Click OK. 7. Repeat Steps 4 through 6 for each caller ID to be accepted on the dialer interface. 	<ol style="list-style-type: none"> 1. Enter edit unit 0 2. Enter edit dialer-options 3. Enter set incoming-map caller 4085550115 4. Repeat Step 3 for each caller ID to be accepted on the dialer interface.

Configuring CHAP on Dialer Interfaces (Optional)

You can optionally configure dialer interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP). When you enable CHAP on a dialer interface, the device can authenticate the remote locations connecting to the USB modem.

For more information about CHAP, see the *JUNOS Software Interfaces and Routing Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.

To configure CHAP on the dialer interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 89 on page 76.
3. If you are finished configuring the device, commit the configuration.
4. To verify the CHAP configuration, see “Verifying the USB Modem Configuration” on page 80.

Table 89: Configuring CHAP on Dialer Interfaces

Task	J-Web Configuration Editor	CLI Configuration Editor
Define a CHAP access profile—for example, <code>usb-modem-access-profile</code> with a client (username) named <code>usb-modem-user</code> and the secret (password) <code>my-secret</code> .	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Access, click Configure or Edit. 3. Next to Profile, click Add new entry. 4. In the Profile name box, type <code>usb-modem-access-profile</code>. 5. Next to Client, click Add new entry. 6. In the Name box, type <code>usb-modem-user</code>. 7. In the Chap secret box, type <code>my-secret</code>. 8. Click OK. 9. Repeat Steps 5 through 8 for each client to be included in the CHAP profile. 10. Click OK until you return to the Configuration page. 	<ol style="list-style-type: none"> 1. From the [edit] hierarchy level, enter <code>edit access</code> 2. Enter <code>set profile usb-modem-access-profile</code> <code>client usb-modem-user chap-secret</code> <code>my-secret</code> 3. Repeat Step 2 for each client to be included in the CHAP profile.
Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, <code>d10 unit 0</code> .	<ol style="list-style-type: none"> 1. On the Configuration page next to Interfaces, click Edit. 2. In the Interface name column, click d10. 3. Under Unit, in the Interface unit number column, click 0. 	From the [edit] hierarchy level, enter <code>edit interfaces d10 unit 0</code>
Configure CHAP on the dialer interface and specify a unique profile name containing a client list and access parameters—for example, <code>usb-modem-access-profile</code> . NOTE: Do not configure the passive option from the [edit interfaces d10 unit 0 ppp-options chap] hierarchy level.	<ol style="list-style-type: none"> 1. Next to Ppp options, click Configure. 2. Next to Chap, click Configure. 3. In the Access profile box, type <code>usb-modem-access-profile</code>. 4. Click OK. 	Enter <code>set ppp-options chap access-profile</code> <code>usb-modem-access-profile</code>

Connecting to the Device from the User End



NOTE: These instructions describe connecting to the device from a remote PC or laptop computer running Microsoft Windows XP. If your remote PC or laptop computer does not run Microsoft Windows XP, see the documentation for your operating system and enter equivalent commands.

This section contains the following topics:

- Configuring a Dial-Up Modem Connection at the User End on page 77
- Connecting to the Device from the User End on page 78

Configuring a Dial-Up Modem Connection at the User End

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 at the user end:

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 is displayed.

4. Click **Create a new connection**.

The New Connection Wizard is displayed.

5. Click **Next**.

The New Connection Wizard: Network Connection Type page is displayed.

6. Select **Connect to the network at my workplace**, and then click **Next**.

The New Connection Wizard: Network Connection page is displayed.

7. Select **Dial-up connection**, and then click **Next**.

The New Connection Wizard: Connection Name page is displayed.

8. In the Company Name box, type the dial-up connection name—for example, **USB-modem-connect**—and then click **Next**.

The New Connection Wizard: Phone Number to Dial page is displayed.

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 is displayed.

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. For information about configuring CHAP on dialer interfaces, see “Configuring CHAP on Dialer Interfaces (Optional)” on page 75.
12. Click **Properties**.

The USB-modem-connect Properties page is displayed.

13. In the Networking tab, select **Internet Protocol (TCP/IP)**, and then click **Properties**.

The Internet Protocol (TCP/IP) Properties page is displayed.

14. Click **Advanced**.

The Advanced TCP/IP Settings page appears.

15. Clear the **Use IP header compression** check box.

Connecting to the Device from the User End

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 is displayed.

2. Double-click the **USB-modem-connect** dial-up connection configured in “Configuring a Dial-Up Modem Connection at the User End” on page 77.

The Connect USB-modem-connect page is displayed.

3. Click **Dial** to connect to the J Series or SRX Series device.

When the connection is complete, you can use Telnet or SSH to connect to the device.

Administering USB Modems

This section contains the following topics:

- Modifying USB Modem Initialization Commands on page 79
- Resetting USB Modems on page 80

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 J-Web or 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.

In this example, you 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. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 90 on page 79.
3. If you are finished configuring the device, commit the configuration.
4. To verify that the initialization commands are configured correctly, see “Verifying the USB Modem Configuration” on page 80.

Table 90: Modifying USB Modem Initialization Commands

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Interfaces, click Configure or Edit. 	From the [edit] hierarchy level, enter edit interfaces umd0

Table 90: Modifying USB Modem Initialization Commands (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the modem AT commands to initialize the USB modem. For example: <ul style="list-style-type: none">■ The command <code>S0=2</code> configures the modem to automatically answer calls on the second ring.■ The command <code>L2</code> configures medium speaker volume on the modem.	<ol style="list-style-type: none">1. Next to Modem options, click Configure.2. In the Init command string box, type <code>AT S0=2 L2</code>.3. Click OK.	From the [edit interfaces umd0] hierarchy, enter <code>set modem-options init-command-string "AT S0=2 L2 \n"</code>
You can insert spaces between commands.		
When you configure modem commands in the CLI configuration editor, you must follow these conventions:		
<ul style="list-style-type: none">■ Use the newline character <code>\n</code> to indicate the end of a command sequence.■ Enclose the command string in double quotation marks.		

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:

1. Enter operational mode in the CLI.
2. To reset the USB modem, enter the following command:

```
user@host> request interface modem reset umd0
```

Verifying the USB Modem Configuration

To verify a USB modem configuration, perform the following tasks:

- Verifying a USB Modem Interface on page 81
- Verifying Dialer Interface Configuration on page 82

Verifying a USB Modem Interface

Purpose Verify that the USB modem interface is correctly configured and display the status of the modem.

Action From the CLI, enter the `show interfaces extensive` command.

Sample Output

```
user@host> show interfaces umd0 extensive

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
```

Meaning The output shows a summary of interface information and displays the modem status.

Verify the following information:

- The physical interface is **Enabled**. If the interface is shown as **Disabled**, do either of the following:
 - In the CLI configuration editor, delete the **disable** statement at the `[edit interfaces interface-name]` level of the configuration hierarchy.

- In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces > *interface-name*** page.
- The physical link is **Up**. A link state of **Down** indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.
- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the **clear interfaces statistics *interface-name*** command.
- The modem initialization command string has a nonzero value for the **S0=*n*** modem command. A nonzero value is required to configure the modem to automatically answer calls. For example, the command **S0=2** configures the modem to automatically answer calls on the second ring.

For more information, see “Modifying USB Modem Initialization Commands” on page 79.

- The modem initialization status is **Ok**. If the initialization status is shown as **Error** or **Not Initialized**, do the following:
 1. Verify that the modem initialization commands are valid. If the modem initialization sequence includes invalid commands, correct them, as described in “Modifying USB Modem Initialization Commands” on page 79.
 2. If the modem initialization commands are valid, reset the modem. For more information, see “Resetting USB Modems” on page 80.

Determine the following information:

- The call status
- The duration of the call

Related Topics For a complete description of **show interfaces** extensive output, see the *JUNOS Interfaces Command Reference*.

Verifying Dialer Interface Configuration

Purpose Verify that the dialer interface is correctly configured.

Action From the CLI, enter the **show interfaces** extensive command.

Sample Output

```
user@host> show interfaces d10 extensive
Physical interface: d10, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
  Device flags      : Present Running
  Interface flags:  SNMP-Traps
  Link type        : Full-Duplex
  Link flags       : Keepalives
```

```

Physical info : Unspecified
Hold-times   : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes :          13859          0 bps
Output bytes :           0          0 bps
Input packets:          317          0 pps
Output packets:           0          0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runt: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0

Logical interface 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

```

Meaning The output shows a summary of dialer interface information. Verify the following information:

- The physical interface is **Enabled**. If the interface is shown as **Disabled**, do either of the following:
 - In the CLI configuration editor, delete the **disable** statement at the [edit **interfaces** *interface-name*] level of the configuration hierarchy.
 - In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces > *interface-name*** page.
- The physical link is **Up**. A link state of **Down** indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates possible link-layer errors.
- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the **clear interfaces statistics *interface-name*** command.
- The dialer state is **Active** when a USB modem call is in progress.
- The LCP state is **Opened** when a USB modem call is in progress. An LCP state of **Closed** or **Not Configured** indicates a problem with the dialer configuration that needs to be debugged with the **monitor traffic interface *interface-name*** command. For information about the **monitor traffic** command, see “Using the monitor traffic Command” on page 375.

Related Topics For a complete description of **show interfaces dl0** extensive output, see the *JUNOS Interfaces Command Reference*.

Chapter 9

Configuring SNMP for Network Management

The Simple Network Management Protocol (SNMP) enables the monitoring of network devices from a central location.

You can use either J-Web Quick Configuration or a configuration editor to configure SNMP.



NOTE: SNMP is not supported on Gigabit Ethernet interfaces on J Series Services Routers.

For more information about SNMP, see the *JUNOS Network Management Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- SNMP Architecture on page 85
- Before You Begin on page 88
- Configuring SNMP with Quick Configuration on page 88
- Configuring SNMP with a Configuration Editor on page 93
- Verifying the SNMP Configuration on page 97

SNMP Architecture

Use SNMP to determine where and when a network failure is occurring, and to gather statistics about network performance in order to evaluate the overall health of the network and identify bottlenecks.

Because SNMP is a client/server protocol, SNMP nodes can be classified as either clients (SNMP managers) or servers (SNMP agents). SNMP managers, also called network management systems (NMSs), occupy central points in the network and actively query and collect messages from SNMP agents in the network. SNMP agents are individual processes running on network nodes that gather information for a particular node and transfer the information to SNMP managers as queries are

processed. The agent also controls access to the agent's Management Information Base (MIB), the collection of objects that can be viewed or changed by the SNMP manager. Because SNMP agents are individual SNMP processes running on a host, multiple agents can be active on a single network node at any given time.

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, and 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, and 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.

Management Information Base

Agents store information in a hierarchical database called the Structure of Management Information (SMI). The SMI resembles a file system. Information is stored in individual files that are hierarchically arranged in the database. The individual files that store the information are known as Management Information Bases (MIBs). Each MIB contains nodes of information that are stored in a tree structure. Information branches down from a root node to individual leaves in the tree, and the individual leaves comprise the information that is queried by managers for a given MIB. The nodes of information are identified by an object ID (OID). The OID is a dotted integer identifier (1.3.6.1.2.1.2, for instance) or a subtree name (such as **interfaces**) that corresponds to an indivisible piece of information in the MIB.

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, <http://www.ietf.org>, and compile them into your NMS, if necessary.

For a list of standard and enterprise-specific supported MIBs, see the *JUNOS Network Management Configuration Guide*.

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.

To download enterprise MIBs for a device, go to http://www.juniper.net/techpubs/software/index_mibs.html.

SNMP Communities

You can grant access to only specific SNMP managers for particular SNMP agents by creating SNMP communities. The community is assigned a name that is unique on the host. All SNMP requests that are sent to the agent must be configured with the same community name. When multiple agents are configured on a particular host,

the community name process ensures that SNMP requests are sorted to only those agents configured to handle the requests.

Additionally, communities allow you to specify one or more addresses or address prefixes to which you want to either allow or deny access. By specifying a list of clients, you can control exactly which SNMP managers have access to a particular agent.

SNMP Traps

The `get` and `set` commands that SNMP uses are useful for querying hosts within a network. However, the commands do not provide a means by which events can trigger a notification. For instance, if a link fails, the health of the link is unknown until an SNMP manager next queries that agent.

SNMP traps are unsolicited notifications that are triggered by events on the host. When you configure a trap, you specify the types of events that can trigger trap messages, and you configure a set of targets to receive the generated messages.

SNMP traps enable an agent to notify a network management system (NMS) of significant events. You can configure an event policy action that uses system log messages to initiate traps for events. The traps enable an SNMP trap-based application to be notified when an important event occurs. You can convert any system log message that has no corresponding traps into a trap. This feature helps you to use NMS traps rather than system log messages to monitor the network.

Spoofing SNMP Traps

You can use the `request snmp spoof-trap` operational mode command to mimic SNMP trap behavior. The contents of the traps (the values and instances of the objects carried in the trap) can be specified on the command line or they can be spoofed automatically. This feature is useful if you want to trigger SNMP traps and ensure they are processed correctly within your existing network management infrastructure, but find it difficult to simulate the error conditions that trigger many of the traps on the device. For more information, see the *JUNOS System Basics and Services Command Reference*.

SNMP Health Monitor

The SNMP health monitor feature uses existing SNMP remote monitoring (RMON) alarms and traps to monitor a select set of services router characteristics (object instances) like the CPU usage, memory usage, and file system usage. The health monitor feature also monitors the CPU usage of the device's forwarding process (also called a daemon)—for example, the chassis process and forwarding process microkernel. You can configure the SNMP health monitor options rising threshold, falling threshold, and interval using the SNMP Quick Configuration page.

A threshold is a test of some SNMP variable against some value, with a report when the threshold value is exceeded. The rising threshold is the upper threshold for a 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, the SNMP health monitor generates an alarm. After the rising alarm, the health monitor

cannot generate another alarm until the sampled value falls below the rising threshold and reaches the falling 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, the SNMP health monitor generates an alarm. After the falling alarm, the health monitor cannot generate another alarm until the sampled value rises above the falling threshold and reaches the rising threshold.

The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

At present, you do not have to configure a separate trap for the SNMP health monitor, because it uses the already existing RMON traps. For more information about RMON events and alarms, see the *JUNOS Network Management Configuration Guide*.

To display the information collected by the SNMP health monitor, use the following CLI `show snmp health-monitor` commands:

- `show snmp health-monitor`
- `show snmp health-monitor alarms`
- `show snmp health-monitor alarms detail`
- `show snmp health-monitor logs`

For more information, see the *JUNOS System Basics and Services Command Reference*.

Before You Begin

Before you begin configuring SNMP, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See the *JUNOS Software Interfaces and Routing Configuration Guide*.

Configuring SNMP with Quick Configuration

J-Web Quick Configuration allows you to define system identification information, create SNMP communities, create SNMP trap groups, and configure health monitor options. Figure 2 on page 89 shows the Quick Configuration page for SNMP.

Figure 2: Quick Configuration Page for SNMP

[Configuration](#) > [Quick Configuration](#) > [SNMP](#)

Quick Configuration

SNMP

Identification

Contact Information
System Description
Local Engine ID
System Location
System Name Override

Communities

No SNMP communities are defined.

Trap Groups

No SNMP trap groups are defined.

Health Monitoring

Enable Health Monitoring ☐ ?
Interval ? (5)
Rising Threshold ? (80)
Falling Threshold ? (70)

To configure SNMP features with Quick Configuration:

1. In the J-Web user interface, select **Configure > Services > SNMP**.
2. Enter information into the Quick Configuration page for SNMP, as described in Table 91 on page 90.
3. From the SNMP Quick Configuration page, click one of the following buttons:
 - To apply the configuration and stay on the Quick Configuration page for SNMP, click **Apply**.
 - To apply the configuration and return to the Quick Configuration SNMP page, click **OK**.
 - To cancel your entries and return to the Quick Configuration for SNMP page, click **Cancel**.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 97.

Table 91: SNMP Quick Configuration Summary

Field	Function	Your Action
Identification		
Contact Information	Free-form text string that specifies an administrative contact for the system.	Type any contact information for the administrator of the system (such as name and phone number).
System Description	Free-form text string that specifies a description for the system.	Type any system information that describes the system (<i>J4350 with 4 PIMs</i> , for example).
Local Engine ID	Provides an administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.	Type the MAC address of Ethernet management port 0.
System Location	Free-form text string that specifies the location of the system.	Type any location information for the system (lab name or rack name, for example).
System Name Override	Free-form text string that overrides the system hostname.	Type the name of the system.
Communities		Click Add .
Community Name	Specifies the name of the SNMP community.	Type the name of the community being added.
Authorization	Specifies the type of authorization (either read-only or read-write) for the SNMP community being configured.	Select the desired authorization (either read-only or read-write) from the list.
Traps		Click Add .
Trap Group Name	Specifies the name of the SNMP trap group being configured.	Type the name of the SNMP trap group being configured.

Table 91: SNMP Quick Configuration Summary (continued)

Field	Function	Your Action
Categories	Specifies which trap categories are added to the trap group being configured.	<ul style="list-style-type: none"> ■ To generate traps for authentication failures, select Authentication. ■ To generate traps for chassis and environment notifications, select Chassis. ■ To generate traps for configuration changes, select Configuration. ■ To generate traps for link-related notifications (up-down transitions), select Link. ■ To generate traps for remote operation notifications, select Remote operations. ■ To generate traps for remote network monitoring (RMON), select RMON alarm. ■ To generate traps for routing protocol notifications, select Routing. ■ To generate traps on system warm and cold starts, select Startup. ■ To generate traps on Virtual Router Redundancy Protocol (VRRP) events (such as new-master or authentication failures), select VRRP events.
Targets	One or more hostnames or IP addresses that specify the systems to receive SNMP traps generated by the trap group being configured.	<ol style="list-style-type: none"> 1. Enter the hostname or IP address, in dotted decimal notation, of the target system to receive the SNMP traps. 2. Click Add.
Health Monitoring		

Table 91: SNMP Quick Configuration Summary (continued)

Field	Function	Your Action
Enable Health Monitoring	<p>Enables the SNMP health monitor on the device. The health monitor periodically (the time you specify in the interval field) checks the following key indicators of device health:</p> <ul style="list-style-type: none"> ■ Percentage of file storage used ■ Percentage of Routing Engine CPU used ■ Percentage of Routing Engine memory used ■ Percentage of memory used for each system process ■ Percentage of CPU used by the forwarding process ■ Percentage of memory used for temporary storage by the forwarding process 	<p>Select the check box to enable the health monitor and configure options. If you do not select the check box, the health monitor is disabled.</p> <p>NOTE: If you select only the Enable Health Monitoring check box and do not specify the options, then SNMP health monitoring is enabled with the default values for the options.</p>
Interval	<p>Determines the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds.</p> <p>For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.</p>	<p>Enter an interval time, in seconds, between 1 and 2147483647.</p> <p>The default value is 300 seconds (5 minutes).</p>
Rising Threshold	<p>Value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is <i>increasing</i>.</p> <p>For example, if the rising threshold is 90 (the default), SNMP generates an event when the value of any key indicator reaches or exceeds 90 percent.</p>	<p>Enter a value between 0 and 100.</p> <p>The default value is 90.</p>
Falling Threshold	<p>Value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is <i>decreasing</i>.</p> <p>For example, if the falling threshold is 80 (the default), SNMP generates an event when the value of any key indicator falls back to 80 percent or less.</p>	<p>Enter a value between 0 and 100.</p> <p>The default value is 80.</p> <p>NOTE: The falling threshold value must be less than the rising threshold value.</p>

Configuring SNMP with a Configuration Editor

To configure SNMP on a services router, you must perform the following tasks marked *(Required)*. For information about using the J-Web and CLI configuration editors, see “User Interface Overview” on page 23.

- Defining System Identification Information (Required) on page 93
- Configuring SNMP Agents and Communities (Required) on page 94
- Managing SNMP Trap Groups (Required) on page 95
- Controlling Access to MIBs (Optional) on page 96

Defining System Identification Information (Required)

Basic system identification information for a services router can be configured with SNMP and stored in various MIBs. This information can be accessed through SNMP requests and either queried or reset. Table 92 on page 93 identifies types of basic system identification and the MIB object into which each type is stored.

Table 92: System Identification Information and Corresponding MIB Objects

System Information	MIB
Contact	sysContact
System location	sysLocation
System description	sysDescr
System name override	sysName

To configure basic system identification for SNMP:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure basic system information using SNMP, perform the configuration tasks described in Table 93 on page 93.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 97.

Table 93: Configuring Basic System Identification

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the SNMP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Snmp, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit snmp</p>

Table 93: Configuring Basic System Identification (*continued*)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the system contact information (such as a name and phone number).	In the Contact box, type the contact information as a free-form text string.	Set the contact information: <code>set contact "contact-information"</code>
Configure the system location information (such as a lab name and a rack name).	In the Location box, type the location information as a free-form text string.	Set the location information: <code>set location "location-information"</code>
Configure the system description (<i>J4350 with 4 PIMs</i> , for example).	In the Description box, type the description information as a free-form text string.	Set the description information: <code>set description "description-information"</code>
Configure a system name to override the system hostname defined in the Getting Started Guide for your device.	In the System Name box, type the system name as a free-form text string.	Set the system name: <code>set name name</code>
Configure the local engine ID to use the MAC address of Ethernet management port 0 as the engine ID suffix.	<ol style="list-style-type: none"> 1. Select Engine id. 2. In the Engine id choice box, select Use mac address from the list. 3. Click OK. 	Set the engine ID to use the MAC address: <code>set engine-id use-mac-address</code>

Configuring SNMP Agents and Communities (Required)

To configure the SNMP agent, you must enable and authorize the network management system access to the services router, by configuring one or more communities. Each community has a community name, an authorization, which determines the kind of access the network management system has to the device, and, when applicable, a list of valid clients that can access the device.

To configure SNMP communities:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure SNMP communities, perform the configuration tasks described in Table 94 on page 94.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 97.

Table 94: Configuring SNMP Agents and Communities

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the SNMP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Snmp, click Configure or Edit. 	From the [edit] hierarchy level, enter <code>edit snmp</code>

Table 94: Configuring SNMP Agents and Communities (*continued*)

Task	J-Web Configuration Editor	CLI Configuration Editor
Create and name a community.	<ol style="list-style-type: none"> Next to Community, click Add new entry. In the Community box, type the name of the community as a free-form text string. 	<p>Create a community:</p> <pre>set community community-name</pre>
Grant read-write access to the community.	In the Authorization box, select read-write from the list.	<p>Set the authorization to read-write:</p> <pre>set community community-name authorization read-write</pre>
Allow community access to a client at a particular IP address—for example, at IP address 10.10.10.10.	<ol style="list-style-type: none"> Next to Clients, click Add new entry. In the Prefix box, type the IP address, in dotted decimal notation. Click OK. 	<p>Configure client access for the IP address 10.10.10.10:</p> <pre>set community community-name clients 10.10.10.10</pre>
Allow community access to a group of clients—for example, all addresses within the 10.10.10.0/24 prefix, except those within the 10.10.10.10/29 prefix.	<ol style="list-style-type: none"> Next to Clients, click Add new entry. In the Prefix box, type the IP address prefix 10.10.10.0/24, and click OK. Next to Clients, click Add new entry. In the Prefix box, type the IP address prefix 10.10.10.10/29. Select the Restrict check box. Click OK. 	<ol style="list-style-type: none"> Configure client access for the IP address 10.10.10.0/24: <pre>set community community-name clients 10.10.10.0/24</pre> Configure client access to restrict the IP addresses 10.10.10.10/29: <pre>set community community-name clients 10.10.10.10/29 restrict</pre>

Managing SNMP Trap Groups (Required)

SNMP traps are unsolicited notifications that are generated by conditions on the services router. When events trigger a trap, a notification is sent to the configured clients for that particular trap group. To manage a trap group, you must create the group, specify the types of traps that are included in the group, and define one or more targets to receive the trap notifications.

To configure SNMP trap groups:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- To configure SNMP trap groups, perform the configuration tasks described in Table 95 on page 96.
- If you are finished configuring the network, commit the configuration.
- To check the configuration, see “Verifying the SNMP Configuration” on page 97.

Table 95: Configuring SNMP Trap Groups

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the SNMP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Snmp, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p><code>edit snmp</code></p>
Create a trap group.	<ol style="list-style-type: none"> 1. Next to Trap group, click Add new entry. 2. In the Group name box, type the name of the group as a free-form text string. 	<p>Create a community:</p> <p><code>set trap-group trap-group-name</code></p>
Configure the trap group to send all trap notifications to a target IP address—for example, to the IP address 192.174.6.6 .	<ol style="list-style-type: none"> 1. Next to Targets, click Add new entry. 2. In the Target box, type the IP address 192.174.6.6, and click OK. 	<p>Set the trap-group target to 192.174.6.6:</p> <p><code>set trap-group trap-group-name targets 192.174.6.6</code></p>
Configure the trap group to generate SNMP notifications on authentication failures, environment alarms, and changes in link state for any of the interfaces.	<ol style="list-style-type: none"> 1. Click Categories. 2. Select the Authentication, Chassis, and Link check boxes. 3. Click OK. 	<p>Configure the trap group categories:</p> <p><code>set trap-group trap-group-name categories authentication chassis link</code></p>

Controlling Access to MIBs (Optional)

By default, an SNMP community is granted access to all MIBs. To control the MIBs to which a particular community has access, configure SNMP views that include the MIBs you want to explicitly grant or deny access to.

To configure SNMP views:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure SNMP views, perform the configuration tasks described in Table 96 on page 96.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 97.

Table 96: Configuring SNMP Views

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the SNMP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Snmp, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p><code>edit snmp</code></p>

Table 96: Configuring SNMP Views (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Create a view.	<ol style="list-style-type: none"> Next to View, click Add new entry. In the Name box, type the name of the view as a free-form text string. 	Create a view: <code>set view view-name</code>
Configure the view to include a MIB—for example, pingMIB.	<ol style="list-style-type: none"> Next to Oid, click Add new entry. In the Name box, type the OID of the pingMIB, in either dotted integer or subtree name format. In the View action box, select include from the list, and click OK. 	Set the pingMIB OID value and mark it for inclusion: <code>set view view-name oid 1.3.6.1.2.1.80 include</code>
Configure the view to exclude a MIB—for example, jnxPingMIB.	<ol style="list-style-type: none"> Next to Oid, click Add new entry. In the Name box, type the OID of the jnxPingMIB, in either dotted integer or subtree name format. In the View action box, select exclude from the list, and click OK twice. 	Set the jnxPingMIB OID value and mark it for exclusion: <code>set view view-name oid jnxPingMIB exclude</code>
Associate the view with a community.	<ol style="list-style-type: none"> On the Snmp page, under Community, click the name of the community to which you want to apply the view. In the View box, type the view name. Click OK. 	Set the community view: <code>set community community-name view view-name</code>

Verifying the SNMP Configuration

To verify the SNMP configuration, perform the following verification task.

Verifying SNMP Agent Configuration

Purpose	Verify that SNMP is running and that requests and traps are being properly transmitted.
Action	From the CLI, enter the <code>show snmp statistics</code> command.
Sample Output	<pre> user@host> show snmp statistics SNMP statistics: Input: Packets: 246213, Bad versions: 12 , Bad community names: 12, Bad community uses: 0, ASN parse errors: 96, Too bigs: 0, No such names: 0, Bad values: 0, Read onlys: 0, General errors: 0, Total request varbinds: 227084, Total set varbinds: 67, Get requests: 44942, Get nexts: 190371, Set requests: 10712, Get responses: 0, Traps: 0, Silent drops: 0, Proxy drops: 0, Commit pending drops: 0, Throttle drops: 0, V3 Input: Unknown security models: 0, Invalid messages: 0 </pre>

```

Unknown pdu handlers: 0, Unavailable contexts: 0
Unknown contexts: 0, Unsupported security levels: 1
Not in time windows: 0, Unknown user names: 0
Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
Output:
Packets: 246093, Too bigs: 0, No such names: 31561,
Bad values: 0, General errors: 2,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 246025, Traps: 0

```

Meaning The output shows a list of the SNMP statistics, including details about the number and types of packets transmitted. Verify the following information:

- The number of requests and traps is increasing as expected with the SNMP client configuration.
- Under **Bad community names**, the number of bad (invalid) communities is not increasing. A sharp increase in the number of invalid community names generally means that one or more community strings are configured incorrectly.

Related Topics For a complete description of `show snmp` statistics output, see the *JUNOS System Basics and Services Command Reference*.

Verifying SNMP Health Monitor Configuration

Purpose Verify that the SNMP health monitor thresholds are set correctly and that the health monitor is operating properly.

Action From the CLI, enter the `show snmp health-monitor` command.

Sample Output `user@host> show snmp health-monitor`

Alarm Index	Variable description	Value	State
32768	Health Monitor: root file system utilization jnxHrStoragePercentUsed.1	70	active
32769	Health Monitor: /config file system utilization jnxHrStoragePercentUsed.2	0	active
32770	Health Monitor: RE 0 CPU utilization jnxOperatingCPU.9.1.0.0	20	active
32772	Health Monitor: RE 0 memory utilization jnxOperatingBuffer.9.1.0.0	95	rising threshold
32774	Health Monitor: jkernel daemon memory usage		
	Init daemon	912	active
	Chassis daemon	93356	active
	Firewall daemon	2244	active
	Interface daemon	3340	active
	SNMP daemon	4412	active
	MIB2 daemon	3920	active
	VRRP daemon	2724	active
	Alarm daemon	1868	active
	PFE daemon	2656	active
	CRAFT daemon	2064	active

```

Traffic sampling control daemon          3320 active
Remote operations daemon                 3020 active
CoS daemon                             3044 active
Inet daemon                             1304 active
Syslog daemon                           1344 active
Web management daemon                   3264 active
USB Supervise Daemon                    1100 active
PPP daemon                              2076 active
DLSWD daemon                            10240 active

32775 Health Monitor: jroute daemon memory usage
Routing protocol daemon                  8952 active
Management daemon                       14516 active
Management daemon                       14556 active
Management daemon                       14556 active
Command line interface                   10312 active
Command line interface                   10312 active
Periodic Packet Management daemon        1640 active
Bidirectional Forwarding Detection daemon 1912 active
L2 Address Learning daemon               2080 active

32776 Health Monitor: jcrypto daemon memory usage
IPSec Key Management daemon              5672 active

32778 Health Monitor: FWDD Micro-Kernel threads total CPU Utilization
jnxFwddMicroKernelCPUUsage.0            0 active

32779 Health Monitor: FWDD Real-Time threads total CPU Utilization
jnxFwddRtThreadsCPUUsage.0              15 active

32780 Health Monitor: FWDD DMA Memory utilization
jnxFwddDmaMemUsage.0                    16 active

32781 Health Monitor: FWDD Heap utilization
jnxFwddHeapUsage.0                       54 active

---(more)---
```

Meaning The output shows a summary of SNMP health monitor alarms and corresponding log entries:

- **Alarm Index**—Alarm identifier.
- **Variable description**—Object instance being monitored.
- **Value**—Current value of the monitored variable in the most recent sample interval.
- **State**—Status of the alarm. For example:
 - **active**—Entry is fully configured and activated.
 - **falling threshold crossed**—Variable value has crossed the lower threshold limit.
 - **rising threshold crossed**—Variable value has crossed the upper threshold limit.

Verify that any rising threshold values are greater than the configured rising threshold, and that any falling threshold values are less than the configured falling threshold.

Related Topics For a complete description of `show snmp health-monitor` output, see the *JUNOS System Basics and Services Command Reference*.

Chapter 10

Configuring the Device for DHCP

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 J Series or SRX Series 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.

You can use J-Web Quick Configuration or a configuration editor to configure DHCP on the device.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- DHCP Terms on page 101
- DHCP Overview on page 102
- Before You Begin on page 104
- Configuring DHCP with Quick Configuration on page 105
- Configuring DHCP with a Configuration Editor on page 116
- Verifying a DHCP Configuration on page 122

DHCP Terms

Before configuring the DHCP server on J Series or SRX Series device, become familiar with the terms defined in Table 97 on page 102.

Table 97: DHCP Terms

Term	Definition
binding	Collection of configuration parameters, including at least an IP address, assigned by a DHCP server to a DHCP client. A binding can be dynamic (temporary) or static (permanent). Bindings are stored in the DHCP server's binding database.
conflict	Problem that occurs when an address within the IP address pool is being used by a host that does not have an associated binding in the DHCP server's database. Addresses with conflicts are removed from the pool and logged in a conflicts list until you clear the list.
DHCP client	Host that uses DHCP to obtain an IP address and configuration settings.
DHCP options	Configuration settings sent within a DHCP message from a DHCP server to a DHCP client. For a list of DHCP options, see RFC 2132, <i>DHCP Options and BOOTP Vendor Extensions</i> .
DHCP server	Host that provides an IP address and configuration settings to a DHCP client. The J Series or SRX Series device is a DHCP server.
Dynamic Host Configuration Protocol (DHCP)	Configuration management protocol you can use to supervise and automatically distribute IP addresses and deliver configuration settings to client hosts from a central DHCP server. An extension of BOOTP, DHCP is defined in RFC 2131, <i>Dynamic Host Configuration Protocol (DHCP)</i> .
gateway router	Device that passes DHCP messages between DHCP clients and DHCP servers. A gateway router is sometimes referred to as a relay agent.
IP address pool	Collection of IP addresses maintained by the DHCP server for assignment to DHCP clients. The address pool is associated with a subnet on either a logical or physical interface.
lease	Period of time during which an IP address is allocated, or bound, to a DHCP client. A lease can be temporary (dynamic binding) or permanent (static binding).
router solicitation address	IP address to which a DHCP client can transmit router solicitation requests.
Windows Name Service (WINS) server	Server running the Microsoft Windows name resolution service for network basic input/output system (NetBIOS) names. WINS is used by hosts running NetBIOS over TCP/IP (NetBT) to register NetBIOS names and to resolve NetBIOS names to IP addresses.

DHCP Overview

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 J Series or SRX Series device can act as a DHCP Server, a DHCP relay agent, or DHCP client 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.

DHCP Server Operation

As a DHCP server, a J Series or SRX Series device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. J Series and SRX Series 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.

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 (J Series or SRX Series 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

J Series and SRX Series device DHCP server functions 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.

DHCP Client Operation

A J Series or SRX Series 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.

Propagation of TCP/IP Settings

The J Series or SRX Series 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 Relay Operation

A J Series or SRX Series device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

For more information, see the *JUNOS Policy Framework Configuration Guide*

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.

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).

Before You Begin

Before you begin configuring the device as a DHCP server, complete the following tasks:

- 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 routers on your network—DNS, NetBIOS servers, boot servers, and gateway routers, for example.
- Determine the DHCP options required by the subnets and clients in your network.

Configuring DHCP with Quick Configuration

This section contains the following topics:

- Configuring DHCP Service with Quick Configuration on page 105
- Configuring the Device as a DHCP Client with Quick Configuration on page 111
- Configuring BOOTP or DHCP Relay with Quick Configuration on page 113

Configuring DHCP Service with Quick Configuration

The DHCP Quick Configuration pages allow you to set up the DHCP service on the device. From the DHCP Service Quick Configuration page, click each of the tabs to configure global settings, DHCP pools for subnets, and static bindings for DHCP clients.

Figure 3 on page 106 through Figure 5 on page 108 show the DHCP Quick Configuration pages.

Figure 3: DHCP Global Settings Quick Configuration Page

[Configuration](#) > [Quick Configuration](#) > [DHCP](#)

Quick Configuration

DHCP

Global Settings DHCP Pools Static Bindings

Server Information

Server Identifier ?

Domain Name ?

Next Server ?

Propagate Interface ?

Domain Search ?

Add Delete

Name Servers ?

Add Delete

Gateway Routers ?

Add Delete

WINS Servers ?

Add Delete

Lease Time and Boot Options

Maximum Lease Time ?

Default Lease Time ?

Boot File ?

Boot Server ?

Option Table

?

Code / Type / Value / / Add Delete

OK Cancel Apply

Figure 4: DHCP Pools Quick Configuration Page

[Configuration](#) > [Quick Configuration](#) > [DHCP](#)

Quick Configuration

DHCP

Add a DHCP Pool

DHCP Pool Information

* Address Pool Subnet

?

* Address Range Low

?

* Address Range High

?

Exclude Addresses

?

Add

Delete

⊞ Server Information

⊞ Lease Time

Option Table

?

Figure 5: DHCP Static Bindings Quick Configuration Page

[Configuration](#) > [Quick Configuration](#) > [DHCP](#)

Quick Configuration

DHCP Add a DHCP Static Binding

DHCP Static Binding Information

* DHCP MAC Address ?

Host Name ?

* Fixed Address ?

Client Identifier ?

+ Server Information

+ Boot Options

Option Table

	?
--	---

To configure the DHCP service with Quick Configuration:

1. In the J-Web user interface, select **Configure > Services > DHCP > DHCP Service**.
2. Enter information into the DHCP Service Quick Configuration pages as described in Table 98 on page 109.
3. From the DHCP Service Quick Configuration page, click one of the following buttons:
 - To apply the configuration and stay on the current Quick Configuration page, click **Apply**.
 - To apply the configuration and return to the DHCP Service Quick Configuration main page, click **OK**.
 - To cancel your entries and return to the DHCP Quick Configuration main page, click **Cancel**.
4. To check the configuration, see “Verifying a DHCP Configuration” on page 122.

Table 98: DHCP Service Quick Configuration Summary

Field	Function	Your Action
Configuring Global Settings		
Server Information		
Server Identifier	Specifies the IP address of the DHCP server reported to a client.	Type the IP address of the device. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.
Domain Name	Specifies the domain name that the clients must use to resolve hostnames.	Type the domain name.
Next Server	Specifies the IP address of the next DHCP server that the clients need to contact.	Type the IP address of the next DHCP server.
Propagate Interface	Specifies the name of the interface on the device through which the resolved DHCP queries are propagated to the DHCP pool.	Type the name of the interface.
Domain Search	Specifies the order—from top to bottom—in which clients must append domain names when resolving hostnames using DNS.	Do one of the following: <ul style="list-style-type: none"> ■ To add a domain name, type the name next to the Add button, and click Add. ■ To delete a domain name, select the name in the Domain Search box, and click Delete.
Name Servers	Defines a list of DNS servers the client can use, in order of preference—from top to bottom.	Do one of the following: <ul style="list-style-type: none"> ■ To add a DNS server, type an IP address next to the Add button, and click Add. ■ To remove a DNS server, select the IP address in the Name Servers box, and click Delete.
Gateway Routers	Defines a list of devices on the subnet that are configured as DHCP relay agents, in order of preference—from top to bottom.	Do one of the following: <ul style="list-style-type: none"> ■ To add a relay agent, type an IP address next to the Add button, and click Add. ■ To remove a relay agent, select the IP address in the Gateway Routers box, and click Delete.
WINS Servers	Specifies the name of the SNMP trap group being configured.	Do one of the following: <ul style="list-style-type: none"> ■ To add a NetBIOS name server, type an IP address next to the Add button, and click Add. ■ To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click Delete.

Table 98: DHCP Service Quick Configuration Summary *(continued)*

Field	Function	Your Action
Lease Time		
Maximum Lease Time (seconds)	Specifies the maximum length of time a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)	Type a number between 60 and 1,209,600 (seconds).
Default Lease Time (seconds)	Specifies the length of time a client can hold a lease, for clients that do not request a specific lease length.	Type a number between 60 and 2,419,200 (seconds).
Boot Options		
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Type the path and a file name.
Boot Server	Specifies the TFTP server that provides the initial boot file to the client.	Type the IP address or hostname of the TFTP server.
Option Table		
Code/Type/Value	Defines a list of option codes, types, and values, in order of preference—from top to bottom. It is mandatory to define all the options.	Do the following: <ul style="list-style-type: none"> ■ Option Code—Type a number. ■ Option Type—Select a type from the list corresponding to the code. ■ Option Value—Type a valid option value based on the type.
Configuring DHCP Pools		
DHCP Pools	Enables you to define address pools for DHCP clients.	To configure a new DHCP pool, click Add under DHCP Pools.
Address Pool Subnet (required)	Specifies the pool subnet on which DHCP is configured.	Type an IP address prefix.
Address Range Low (required)	Specifies the lowest address in the IP address pool range.	Type an IP address that is part of the subnet specified in Address Pool Subnet.
Address Range High (required)	Specifies the highest address in the IP address pool range.	Type an IP address that is part of the subnet specified in Address Pool Subnet. This address must be greater than the address specified in Address Range Low.
Exclude Addresses	Specifies addresses to exclude from the IP address pool.	Do one of the following: <ul style="list-style-type: none"> ■ To add an excluded address, type the address next to the Add button, and click Add. ■ To delete an excluded address, select the address in the Exclude Addresses box, and click Delete.
Configuring DHCP Static Bindings		
DHCP Static Bindings	Enables you to assign DHCP clients to static IP addresses.	To configure a new static binding, click Add under DHCP Static Bindings.

Table 98: DHCP Service Quick Configuration Summary *(continued)*

Field	Function	Your Action
DHCP MAC Address (required)	Specifies the MAC address of the client to be permanently assigned a static IP address.	Type the hexadecimal MAC address of the client.
Host Name	Specifies the client hostname associated with its IP address used by the DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides.	Type a client hostname.
Fixed IP Address (required)	Defines a list of IP addresses permanently assigned to the client. A static binding must have at least one fixed address assigned to it, but multiple addresses are also allowed.	Do one of the following: <ul style="list-style-type: none"> ■ To add an IP address, type the address next to the Add button, and click Add. ■ To remove an IP address, select the address in the Fixed IP Addresses box, and click Delete.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The client identifier can be an ASCII or hexadecimal string.	Do either of the following: <ul style="list-style-type: none"> ■ Select the client identifier type from the list. If you select Hexadecimal, you must type the client identifier using numbers 0 through 9, and letters A through F. ■ Type the client identifier.

Configuring the Device as a DHCP Client with Quick Configuration

The DHCP Client Quick Configuration page allows you to configure a server to act as a DHCP client and receive the TCP/IP settings and the IP address for any physical interface.

Figure 6 on page 112 shows the DHCP Client Quick Configuration page.

Figure 6: DHCP Client Quick Configuration Page

[Configuration](#) > [Quick Configuration](#) > [DHCP](#)

Quick Configuration

DHCP Add a DHCP Client

DHCP Client Information

* **Interface** ?

Client Identifier ?

Lease Time ?

Retransmission Attempt ?

Retransmission Interval ?

DHCP Server Address ?

Vendor Class ID ?

Update Server ☐ ?

To configure the DHCP client with Quick Configuration:

1. In the J-Web user interface, select **Configure > Services > DHCP > DHCP Client**.
2. Under DHCP Client, click **Add** and enter information into the DHCP Client Quick Configuration page as described in Table 99 on page 112
3. From the DHCP Client Quick Configuration page, click one of the following buttons:
 - To apply the configuration and stay on the Quick Configuration page for DHCP Client, click **Apply**.
 - To apply the configuration and return to the DHCP Client Quick Configuration main page, click **OK**.
 - To cancel your entries and return to the DHCP Client Quick Configuration main page, click **Cancel**.
4. To check the configuration, see “Verifying the DHCP Client” on page 124.

Table 99: DHCP Client Quick Configuration Summary

Field	Function	Your Action
DHCP Client		
DHCP Client	Enables you to configure the device to operate as a DHCP client.	From the DHCP Quick Configuration page, click Add under DHCP Client.
Interface (required)	Specifies the interface on which to configure the DHCP client.	Type the name of the interface.

Table 99: DHCP Client Quick Configuration Summary *(continued)*

Field	Function	Your Action
Client Identifier	<p>Specifies the name of the client used by the DHCP server to index its database of address bindings.</p> <p>The client identifier can be an ASCII or hexadecimal string.</p>	<p>Do either of the following:</p> <ul style="list-style-type: none"> ■ Select the client identifier type from the list. If you select Hexadecimal, you must type the client identifier using numbers 0 through 9, and letters A through F. ■ Type the client identifier.
Lease Time (seconds)	Specifies the time to negotiate and exchange DHCP messages.	Type a number between 60 and 2,147,483,647 (seconds).
Retransmission Attempt	Specifies the number of attempts the device is allowed to retransmit a DHCP packet fallback.	<p>Type a number between 0 and 6.</p> <p>The default is 4.</p>
Retransmission Interval (seconds)	Specifies the time interval allowed between successive retransmission attempts.	<p>Type a number between 4 and 64.</p> <p>The default is 4.</p>
DHCP Server Address	Specifies the preferred DHCP server the DHCP clients contact with DHCP queries.	Type the IPv4 address of the DHCP server.
Vendor Class ID	Specifies the vendor class identity number for the DHCP client.	Type the vendor class ID.
Update Server	Specifies whether the propagation of TCP/IP settings is enabled on the specified interface (if it is acting as a DHCP client) to the DHCP server configured on the device.	To enable the propagation of TCP/IP settings to the DHCP server configured on the device, select Update Server check box.

Configuring BOOTP or DHCP Relay with Quick Configuration

The Bootp/DHCP Relay Quick Configuration page allows you to configure the device as a relay agent to forward the incoming BOOTP or DHCP requests from BOOTP or DHCP clients to a BOOTP server. Figure 7 on page 114 shows the Bootp/DHCP Relay Quick Configuration page.

Figure 7: Bootp/DHCP Relay Quick Configuration Page

[Configuration](#) > [Quick Configuration](#) > [DHCP](#)

Quick Configuration

DHCP

Bootp/DHCP Relay Information

DHCP Relay Agent ☐ ?

VPN Encryption ☐ ?

Client Response TTL ?

Maximum Hop Count ?

Minimum Waiting Time ?

Description of Servers ?

Servers/Routing Instance ?

/

Interfaces ?

To configure the device as a DHCP relay agent with Quick Configuration:

1. In the J-Web user interface, select **Configure > Services > DHCP > Boot DHCP Relay**.
2. Enter information into the Bootp/DHCP Relay Quick Configuration page as described in Table 100 on page 115
3. From the Bootp/DHCP Relay Quick Configuration page, click one of the following buttons:
 - To apply the configuration and stay on the Quick Configuration page for Bootp/DHCP Relay, click **Apply**.
 - To apply the configuration and return to the previous page, click **OK**.
 - To cancel your entries and return to the previous page, click **Cancel**.
4. To check the configuration, see “Displaying DHCP Relay Statistics” on page 126.

Table 100: Bootp/DHCP Relay Quick Configuration Summary

Field	Function	Your Action
DHCP Relay Agent	Specifies if the DHCP relay agent is enabled to relay BOOTP or DHCP messages to a BOOTP server.	To enable the relay agent, select DHCP Relay Agent check box.
VPN Encryption	Specifies if VPN encryption is enabled to allow client requests to pass through a VPN tunnel.	To enable VPN encryption, select VPN Encryption check box.
Client Response TTL	Specifies the IP time-to-live value, in seconds, to set in responses to clients.	Type a number between 1 and 225.
Maximum Hop Count	Specifies the maximum number of hops allowed per packet.	Type a number between 4 and 16.
Minimum Wait Time	Specifies the minimum number of seconds before requests are forwarded to the BOOTP server.	Type a number between 0 and 30,000.
Description of Server	Specifies the description for the BOOTP server.	Type the description in the Description of the Server text box.
Servers/Routing Instance	Defines a list of IP addresses of the servers and routing instances, in order of preference—from top to bottom.	<ol style="list-style-type: none"> Do the following: <ul style="list-style-type: none"> Type the IP address of the server. Select a routing instance. A routing instance is optional. Do one of the following: <ul style="list-style-type: none"> To add a server, type an IP address next to the Add button, and click Add. To remove a server, select the IP address in the Servers/Routing Instance list, and click Delete.
Interfaces	Defines a list of the incoming BOOTP or DHCP request forwarding interfaces, in order of preference—from top to bottom.	<p>Do one of the following:</p> <ul style="list-style-type: none"> To add a DNS server, type an IP address next to the Add button, and click Add. To remove a DNS server, select the IP address in the Interfaces list, and click Delete.

Configuring DHCP with a Configuration Editor

This section contains the following topics:

- Configuring the Device as a DHCP Server on page 116
- Configuring the Device as a DHCP Client on page 119
- Configuring the Device as a BootP/DHCP Relay Agent on page 120

Configuring the Device as a DHCP Server

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. See RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*, for more information.
- A DNS name server.
- A DHCP option—Router 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 101 on page 116 provides the settings and values for the sample DHCP server configuration used in this section.

Table 101: Sample DHCP Configuration Settings

Settings	Sample Value or Values
DHCP Subnet Configuration	
Address pool subnet address	192.168.2.0/24
High address in the pool range	192.168.2.254
Low address in the pool range	192.168.2.2
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

Table 101: Sample DHCP Configuration Settings (continued)

Settings	Sample Value or Values
Identifier code for router solicitation address option	32
Type choice for router solicitation address option	Ip address
IP address for router solicitation address option	192.168.2.33
DHCP MAC Address Configuration	
Static binding MAC address	01:03:05:07:09:0B
Fixed address	192.168.2.50

To configure the device as a DHCP server for a subnet and a single client:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 102 on page 117.
3. If you are finished configuring the device, commit the configuration.
4. To verify DHCP server configuration and operation, see “Verifying a DHCP Configuration” on page 122.

Table 102: Configuring the Device as a DHCP Server

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Dhcp server level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 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. 	<p>From the [edit] hierarchy level, enter</p> <p>edit system services dhcp</p>
Define the IP address pool.	<ol style="list-style-type: none"> 1. Next to Pool, click Add new entry. 2. In the Subnet address box, type 192.168.2.0/24. 3. Next to Address range, select the check box. 4. Next to Address range, click Configure. 5. In the High box, type 192.168.2.254. 6. In the Low box, type 192.168.2.2. 7. Click OK. 	<p>Set the IP address pool range:</p> <p>set pool 192.168.2.0/24 address-range low 192.168.2.2 high 192.168.2.254</p>

Table 102: Configuring the Device as a DHCP Server *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Define the default and maximum lease times, in seconds.	<ol style="list-style-type: none"> From the Default lease time list, select Enter Specific Value. In the Length box, type 1209600. From the Maximum lease time list, select Enter Specific Value. Next to Maximum lease time, type 2419200. 	Set the default and maximum lease times: <pre>set pool 192.168.2.0/24 default-lease-time 1209600 maximum-lease-time 2419200</pre>
Define the domain search suffixes to be used by the clients.	<ol style="list-style-type: none"> Next to Domain search, click Add new entry. In the Suffix box, type mycompany.net. Click OK. Next to Domain search, click Add new entry. In the Suffix box, type mylab.net. Click OK. 	Set the domain search suffixes: <pre>set pool 192.168.2.0/24 domain-search mycompany.net set pool 192.168.2.0/24 domain-search mylab.net</pre>
Define a DNS server.	<ol style="list-style-type: none"> Next to Name server, click Add new entry. In the Address box, type 192.168.10.2. Click OK. 	Set the DNS server IP address: <pre>set pool 192.168.2.0/24 name-server 192.168.10.2</pre>
Define DHCP option 32—the router solicitation address option.	<ol style="list-style-type: none"> Next to Option, click Add new entry. In the Option identifier code box, type 32. From the Option type choice list, select Ip address. In the Ip address box, type 192.168.2.33. Click OK twice. 	Set the router solicitation IP address: <pre>set pool 192.168.2.0/24 option 32 ip-address 192.168.2.33</pre>
Assign a static IP address of 192.168.2.50 to MAC address 01:03:05:07:09:0B.	<ol style="list-style-type: none"> Next to Static binding, click Add new entry. In the Mac address box, type 01:03:05:07:09:0B. Next to Fixed address, click Add new entry. In the Address box, type 192.168.2.50. Click OK until you return to the Configuration page. 	Associate a fixed IP address with the MAC address of the client: <pre>set static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50</pre>

Configuring the Device as a DHCP Client

To configure the J Series or SRX Series device as a DHCP client:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 103 on page 119.
3. If you are finished configuring the device, commit the configuration.
4. To verify DHCP client configuration and operation, see “Verifying the DHCP Client” on page 124.

Table 103: Configuring the Device as a DHCP Client

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy, and select the interface on which to configure DHCP client information—for example, <code>ge-0/0/1.0</code> .	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 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. 	<p>From the [edit] hierarchy level, enter</p> <pre>set interfaces ge-0/0/1 unit 0 family inet dhcp</pre>
<p>Configure the DHCP client identifier as either an ASCII or hexadecimal value.</p> <p>Use hexadecimal if the client identifier is a MAC address—for example, <code>00:0a:12:00:12:12</code>.</p>	<ol style="list-style-type: none"> 1. Next to Client identifier, click Configure. 2. From the Client identifier choice list, select hexadecimal. 3. In the Hexadecimal box, type the client identifier—<code>00:0a:12:00:12:12</code>. 4. Click OK. 	<p>Set the DHCP client identifier as a hexadecimal value:</p> <pre>set interfaces ge-0/0/1 unit 0 family inet dhcp client-identifier 00:0a:12:00:12:12</pre>
<p>Set the DHCP lease time in seconds—for example, <code>86400</code> (24 hours).</p> <p>The range is 60 through 2147483647 seconds.</p>	<ol style="list-style-type: none"> 1. From the Lease time list, select Enter Specific Value. 2. In the Length box, type <code>86400</code>. 	<p>Set the DHCP lease time to 86400 seconds:</p> <pre>set interfaces ge-0/0/1 unit 0 family inet dhcp lease-time 86400</pre>
<p>Define the number of attempts allowed to retransmit a DHCP packet—for example, <code>6</code>.</p> <p>The range is 0 through 6. The default is 4 times.</p>	<p>In the Retransmission attempt box, type <code>6</code>.</p>	<p>Set the number of attempts allowed to retransmit a DHCP packet to 6:</p> <pre>set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-attempt 6</pre>

Table 103: Configuring the Device as a DHCP Client (*continued*)

Task	J-Web Configuration Editor	CLI Configuration Editor
Define the interval, in seconds, allowed between retransmission attempts—for example, 5. The range is 4 through 64. The default is 4 seconds.	In the Retransmission interval box, type 5.	Set the interval allowed between retransmission attempts to 5 seconds: set interfaces ge-0/0/1 unit 0 family inet dhcp retransmission-interval 5
Set the IPv4 address of the preferred DHCP server—for example, 10.1.1.1.	In the Server address box, type 10.1.1.1.	Set the IPv4 address of the preferred DHCP server to 10.1.1.1: set interfaces ge-0/0/1 unit 0 family inet dhcp server-address 10.1.1.1
Set the vendor class ID for the DHCP client—for example, ether.	1. In the Vendor id box, type ether. 2. Click OK .	Set the vendor class ID to ether: set interfaces ge-0/0/1 unit 0 family inet dhcp vendor-id ether

Configuring the Device as a DHCP Relay Agent

You can configure the device or an interface to act as a DHCP relay agent. Doing so enables the device to respond to DHCP or BOOTP requests broadcast by request as a broadcast message. If the device or an interface detects a broadcast message, it relays the message to a specified DHCP or BOOTP server.

We recommend you to configure the device or an interface to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server. For more information, see *JUNOS Policy Framework Configuration Guide*.

Configuring the Device as a BootP/DHCP Relay Agent

To configure the J Series or SRX Series device as a BootP/DHCP relay agent:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 104 on page 121.
3. If you are finished configuring the device, commit the configuration.
4. To verify DHCP client configuration and operation, see “Displaying DHCP Relay Statistics” on page 126.

Table 104: Configuring the Device as a BootP/DHCP Relay Agent

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Forwarding-options level in the configuration hierarchy, and select the interface on which to configure the BootP/DHCP relay agent information.	In the J-Web interface, select Configure > Services > DHCP > Boot DHCP Relay .	From the [edit] hierarchy level, enter set forwarding-options helpers bootp
Enable the DHCP relay agent to relay bootp/DHCP messages to BootP server.	Select the DHCP relay agent check box to enable the BootP/DHCP relay agent.	Enable the DHCP relay agent: set forwarding-options helpers bootp relay agent-option
Enable VPN encryption to allow client requests to pass through the VPN tunnel.	Select the VPN encryption check box.	Enable VPN encryption to allow client requests to pass through VPN tunnel: set forwarding-options helpers bootp vpn
Define the IP time-to-live value to be set in responses to client—for example, 20. The range is 1—255.	In the Client response TTL box, type 20.	Set the IP time-to-live value to be set in responses to client to 20: set forwarding-options helpers bootp client-response-ttl 20
Define the maximum number of hops allowed per packet—for example, 10. The range is 4—16.	In the Maximum hop count box, type 10.	Set the maximum number of hops allowed per packet to 10: set forwarding-options helpers bootp maximum-hop-count number 10
Define the minimum number of seconds before requests are forwarded—for example, 300. The range is 0—30000 seconds.	In the Minimum wait time box, type 300.	Set the minimum number of seconds before requests are forwarded to 300: set forwarding-options helpers bootp minimum-wait-time seconds 300
Define the text description of the server. The value is a string.	In the Description box, type the description of the server.	Set the description of the server: set forwarding-options helpers bootp description text
Define a valid server name or address to the server to forward. The value is an IPv4 address.	<ol style="list-style-type: none"> Next to Sever, click Add new Entry. Next to the Name box, type 2.2.2.2. 	Set the server name: set forwarding-options helpers bootp server

Table 104: Configuring the Device as a BootP/DHCP Relay Agent *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Define the routing instance. The value is a nonreserved text string of 128 characters or less.	<ol style="list-style-type: none"> Next to Routing instance, click Add new entry. In the Name box, type <code>rt-i-1</code> and click OK. <p>A routing instance is optional.</p>	<p>Set the routing instance:</p> <p>set forwarding-options helpers bootp server routing instance</p>
Define the incoming BootP/DHCP request forwarding interface—for example, <code>ge-0/0/0</code> .	<ol style="list-style-type: none"> Next to Routing instance, click Add new entry. In the Interface name box, type <code>ge-0/0/0</code>. Click OK until you return to the Configuration page. 	<p>Set the incoming BootP/DHCP request forwarding interface to <code>ge-0/0/0</code>:</p> <p>set forwarding-options helpers bootp interface ge-0/0/0</p>

Verifying a DHCP Configuration

To verify a DHCP configuration, perform the following tasks:

- Displaying Global DHCP Information on page 122
- Verifying the DHCP Binding Database on page 123
- Verifying the DHCP Client on page 124
- Verifying DHCP Server Operation on page 125
- Displaying DHCP Relay Statistics on page 126

Displaying Global DHCP Information

Purpose Verify the global DHCP Information

Action From the CLI, enter the `show system services dhcp global` command.

```

user@host> show system services dhcp global
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: englab.juniper.net
  Name: name-server, Value: [ 192.168.5.68, 172.17.28.101, 172.17.28.100 ]

```

Meaning Verify that the output shows the intended global information of the DHCP server.

Related Topics For complete descriptions of the `show system services dhcp` command and output, see the *JUNOS System Basics and Services Command Reference*.

Verifying the DHCP Binding Database

Purpose Verify that the DHCP binding database reflects your DHCP server configuration

Action From operational mode in the CLI, to display all active bindings in the database, enter the **show system services dhcp binding** command. To display more information about a client, including its DHCP options, enter the **show system services dhcp binding address detail** command, replacing *address* with the IP address of the client. Finally, enter the **show system services dhcp conflict** command.

The DHCP binding database resulting from the configuration defined in Table 102 on page 117 is displayed in the following sample output.

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

```

Meaning Verify the following information:

- For each dynamic binding, verify that the IP address is within the range of the configured IP address pool. Under **Lease Expires**, verify that the difference between the date and time when the lease expires and the current date and time is less than the maximum configured lease time.
- For each static binding, verify that the IP address corresponds to the MAC address displayed under **Hardware Address** (as defined in the **static-binding** statement in the configuration). Under **Lease Expires**, verify that the lease expiration is **never**.
- In the output displayed by the **show system services dhcp binding address detail** command, verify that the options under **DHCP options** are correct for the subnet.
- Verify that the **show system services dhcp conflict** command does not display any conflicts.

Related Topics For complete descriptions of the `show system services dhcp` command and output, see the *JUNOS System Basics and Services Command Reference*.

Verifying the DHCP Client

Purpose Verify that the DHCP client information reflects your DHCP client configuration

Action From operational mode in the CLI, to display DHCP client information, enter the `show system services dhcp client` command. To display more information about a specified interface, enter the `show system services dhcp client interface-name` command. Finally, enter the `show system services dhcp client statistics` command.

The DHCP client configuration resulting from the CLI configuration is displayed in the following sample output.

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: englab.juniper.net

user@host> show system services dhcp client statistics
Packets dropped:
Total      0
Messages Received:
DHCP OFFER    0
DHCPACK       8
DHCPNAK       0

Messages Sent:
DHCPDECLINE   0
DHCPDISCOVER  0

```


DHCPREQUEST	1
DHCPINFORM	0
DHCPRELEASE	0
DHCPRENEW	7
DHCPREBIND	0

Meaning Verify whether the DHCP client information reflects your DHCP client configuration.

Related Topics For complete descriptions of the `show system services dhcp client` command and output, see the *JUNOS Software CLI Reference*.

Verifying DHCP Server Operation

Purpose Verify that the DHCP server is operating as configured.

- Action** Take the following actions:
- Use the `ping` command to verify that a client responds to ping packets containing the destination IP address assigned by the device.
 - 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.

Sample Output

```

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

```

- Meaning** Verify the following:
- The client returns a ping response.

- The client IP configuration displayed contains the configured values. For example, for the DHCP configuration in “Configuring the Device as a DHCP Server” on page 116, you can verify the following settings:
 - DNS Suffix Search List is correct.
 - IP address is within the IP address pool you configured.
 - DHCP Server is the primary IP address of the device interface on which the DHCP message exchange occurs. If you include the `server-identifier` statement in your configuration, the DHCP server IP address specified in this statement is displayed.
 - Lease Obtained and Lease Expires times are correct.

The `ipconfig` command also displays other DHCP client settings that can be configured on the device, including the client's hostname, default gateways, and WINS servers.

Related Topics For complete descriptions of the `ping` command and output, see the *JUNOS System Basics and Services Command Reference*.

Displaying DHCP Relay Statistics

Purpose Display DHCP Relay statistics to verify normal operation.

Action Enter the `show system services dhcp relay-statistics` command to display the DHCP relay statistics.

Sample Output

```
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
```

Meaning Verify the following:

- The default settings displayed are consistent with your DHCP server configuration.
- The number of dropped packets and errors is small.
- The reason for the packets being dropped.

Related Topics For complete descriptions of the `show system services dhcp relay-statistics` command and output, see the *JUNOS Software CLI Reference*.

Chapter 11

Configuring Autoinstallation

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 CLI configuration editor to configure a device for autoinstallation. The J-Web interface does not include Quick Configuration pages for autoinstallation.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics:

- Autoinstallation Terms on page 127
- Autoinstallation Overview on page 128
- Before You Begin on page 130
- Configuring Autoinstallation with a Configuration Editor on page 131
- Verifying Autoinstallation on page 133

Autoinstallation Terms

Before configuring autoinstallation, become familiar with the terms defined in Table 105 on page 127.

Table 105: Autoinstallation Terms

Term	Definition
autoinstallation	Automatic configuration of a device over the network from a preexisting configuration file that you create and store on a configuration server—typically a Trivial File Transfer Protocol (TFTP) server. Autoinstallation takes place on a device that is powered on without a valid configuration (boot) file or is configured specifically for autoinstallation. Autoinstallation is useful for deploying multiple devices in a network.
default configuration	Configuration that takes place on a device unable to locate a configuration (boot) file. You can set up two default configuration files for autoinstallation on the device: network.conf to specify IP address-to-hostname mappings for devices on the network, or router.conf to provide just enough configuration for your subsequent Telnet access.
hostname.conf	Host-specific configuration file for autoinstallation on a device that contains all the configuration information necessary for the device. In the filename, hostname is replaced with the hostname you are assigning to the device.

Table 105: Autoinstallation Terms (*continued*)

Term	Definition
host-specific configuration	Configuration that takes place on a device for which you have created a host-specific configuration file for autoinstallation called <i>hostname.conf</i> . The <i>hostname.conf</i> file contains all the information necessary to configure the device. For the device to use <i>hostname.conf</i> , it must be able to determine its own hostname from the network.
network.conf	Default configuration file for autoinstallation, in which you specify IP addresses and associated hostnames for devices on the network.
router.conf	Default configuration file for autoinstallation with a minimum configuration sufficient for you to telnet to the device and configure it manually.

Autoinstallation Overview

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 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 CompactFlash 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 J Series or SRX Series 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 overview contains the following topics:

- Supported Autoinstallation Interfaces and Protocols on page 128
- Typical Autoinstallation Process on a New Device on page 129

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 106 on page 129 lists the protocols that the device can use on these interfaces for IP address acquisition.

Table 106: Interfaces and Protocols for IP Address Acquisition During Autoinstallation

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

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

Typical Autoinstallation Process on a New Device

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

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

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

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

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

- The IP address of an intermediate device if the configuration server is on a different LAN segment from the new device.

2. After the new device acquires an IP address, the autoinstallation process on the device attempts to download a configuration file in the following ways:
 - a. If the DHCP server specifies the host-specific configuration file (boot file) *hostname.conf*, the device uses that filename in the TFTP server request. (In the filename, *hostname* is the hostname of the new device.) The autoinstallation process on the new device makes three unicast TFTP requests for *hostname.conf*. If these attempts fail, the device broadcasts three requests to any available TFTP server for the file.
 - b. If the new device cannot locate *hostname.conf*, the autoinstallation process unicasts or broadcasts TFTP requests for a default device configuration file called *network.conf*, which contains hostname-to-IP address mapping information, to attempt to find its hostname.
 - c. If *network.conf* contains no hostname entry for the new device, the autoinstallation process sends out a DNS request and attempts to resolve the new device's IP address to a hostname.
 - d. If the new device can determine its hostname, it sends a TFTP request for the *hostname.conf* file.
 - e. If the new device is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file *router.conf*.
3. After the new device locates a configuration file on a TFTP server, autoinstallation downloads the file, installs the file on the device, and commits the configuration.

Before You Begin

To configure a network for device autoinstallation, complete the following tasks:

- Configure a DHCP server on your network to meet your network requirements.

You can configure a device to operate as a DHCP server. For more information, see “Configuring the Device for DHCP” on page 101.
- 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

- 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.
- If you are using *hostname.conf* files for autoinstallation of host-specific configuration files, you must also complete the following tasks:
 - Configure the DHCP server to provide a *hostname.conf* filename to each new device. Each device uses its *hostname.conf* filename to request a configuration file from the TFTP server. Copy the necessary *hostname.conf* configuration files to the TFTP server.
 - Create a default configuration file named *network.conf*, and copy it to the TFTP server. This file contains IP address-to-hostname mapping entries. If the DHCP server does not send a *hostname.conf* filename to a new device, the device uses *network.conf* to resolve its hostname based on its IP address.

Alternatively, you can add the IP address-to-hostname mapping entry for the new device to a DNS database file.

The device uses the hostname to request a *hostname.conf* file from the TFTP server.

Configuring Autoinstallation with a Configuration Editor

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.

To configure autoinstallation:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 107 on page 132.
3. If you are using the J-Web interface, click **Commit** to view a summary of your changes, then click **OK** to commit the configuration. If you are using the CLI, commit the configuration by entering the `commit` command.
4. To check the configuration, see “Verifying Autoinstallation” on page 133.

Table 107: Configuring Autoinstallation

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the System level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system
Enable autoinstallation.	Select Autoinstallation , and then click Configure .	Enter set autoinstallation configuration-servers url
Specify the URL address of one or more servers from which to obtain configuration files. For example: <ul style="list-style-type: none"> ■ tftp://tftpconfig.sp.com ■ ftp://user:password@sftpconfig.sp.com 	<ol style="list-style-type: none"> 1. Next to Configuration servers, click Add new entry. 2. Type the location of the configuration server in the Url box. 3. If a password is required for server access, type it into the Password box. 4. Click OK to return to the Autoinstallation page. 	
Configure one or more Ethernet or serial interfaces to perform autoinstallation.	<ol style="list-style-type: none"> 1. Next to Interfaces, click Add new entry. 2. Type the name of the interface into the Interface name box—for example, ge-0/0/0. 3. Click OK. 	To set BOOTP and RARP on an Ethernet interface, enter set autoinstallation interfaces ge-0/0/0 bootp rarp
Configure one or two procurement protocols for each interface. The device uses the protocols to send a request for an IP address for the interface. <ul style="list-style-type: none"> ■ BOOTP—Sends requests over all interfaces. ■ RARP—Sends requests over Ethernet interfaces. ■ SLARP—Sends requests over serial interfaces. 	<ol style="list-style-type: none"> 1. Next to the interface name, click Edit. 2. Select one or two protocols to be used by autoinstallation over the interface—for example, Bootp and Rarp. 3. Click OK. 	



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 via user configuration while the factory default configuration configures CISCO HLDC on the same interface, then the interface might not come up and the following error will be logged in the message file: **“DCD_CONFIG_WRITE_FAILED failed.”**

Verifying Autoinstallation

To verify that a device is configured for autoinstallation, perform the following task.

Verifying Autoinstallation Status

Purpose Display the status of the autoinstallation feature on a device.

Action From the CLI, enter the `show system autoinstallation status` command.

Sample Output

```
user@host> show system autoinstallation status
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  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: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
Interface:
  Name: ge-0/0/1
  State: None
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

Meaning The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the device when it is deployed on the network.

Chapter 12

Automating Network Operations and Troubleshooting

You can use commit scripts, operation scripts, and event policies to automate of network operations and troubleshooting tasks. You can use commit scripts to enforce custom configuration rules. Operation scripts allow you to automate network management and troubleshooting tasks. You can configure event policies that initiate self-diagnostic actions on the occurrence of specific events.

For more information about using commit scripts and operation scripts and configuring event policies, see the *JUNOS Configuration and Diagnostic Automation Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Defining and Enforcing Configuration Rules with Commit Scripts on page 135
- Automating Network Management and Troubleshooting with Operation Scripts on page 138
- Running Self-Diagnostics with Event Policies on page 140

Defining and Enforcing Configuration Rules with Commit Scripts

Being able to restrict network configurations in accordance with custom configuration rules can reduce human error and improve network uptime and reliability. Commit scripts allow you to enforce custom configuration rules.

This section contains the following topics:

- Commit Script Overview on page 135
- Enabling Commit Scripts on page 136
- Disabling Commit Scripts on page 137

Commit Script Overview

Commit scripts run each time a new candidate configuration is committed and inspect the configuration. If a candidate configuration does not adhere to your design rules,

a commit script can instruct the services router to perform various actions, including the following:

- Generate custom warning messages, system log messages, or error messages.

If error messages are generated, the commit operation fails and the candidate configuration remains unchanged.
- Change the configuration in accordance with your rules and then proceed with the commit operation.

Consider the following examples of actions you can perform with commit scripts:

- Run a basic sanity test. Ensure that the `[edit interfaces]` and `[edit protocols]` hierarchies have not been accidentally deleted.
- Check configuration consistency. Ensure that every T1 interface configured at the `[edit interfaces]` hierarchy level is also configured at the `[edit protocols rip]` hierarchy level.
- Enforce network design rules. For example, suppose your network design requires every interface on which the International Organization for Standardization (ISO) family of protocols is enabled to also have Multiprotocol Label Switching (MPLS) enabled. At commit time, a commit script inspects the configuration and issues an error if this requirement is not met. This error causes the commit operation to fail and forces the user to update the configuration to comply.

Instead of an error, the commit script can issue a warning about the configuration problem and then automatically correct it, by changing the configuration to enable MPLS on all interfaces. A system log message can also be generated indicating that corrective action was taken.

The scripting language you use for writing commit scripts is Extensible Stylesheet Language Transformations (XSLT). XSLT commit scripts are based on JUNOScript Extensible Markup Language (XML).

Enabling Commit Scripts

To enable commit scripts:

1. Write a commit script.

For information about writing commit scripts, see the *JUNOS Configuration and Diagnostic Automation Guide*.

2. Copy the script to the `/var/db/scripts/commit` directory.

Only users with superuser privileges can access and edit files in the `/var/db/scripts/commit` directory.

3. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
4. Perform the configuration tasks described in Table 108 on page 137.
5. If you are finished configuring the network, commit the configuration.

Table 108: Enabling Commit Scripts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Commit level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Scripts, click Configure or Edit. 4. Next to Commit, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system scripts commit
Enable the commit script file—for example, commit-script.xml.	<ol style="list-style-type: none"> 1. Next to File, click Add new entry. 2. In the File name box, type commit-script.xml. 3. Click OK. 	Set the script file name: set file commit-script.xml

Disabling Commit Scripts

If you do not want a commit script to run, you can disable it by deleting or deactivating it in the configuration. Deleting a commit script permanently removes it from the configuration. To run the script later, you must reenabling the script as described in “Enabling Commit Scripts” on page 136. Deactivating a commit script disables the script until you activate it later.

To delete a commit script:

1. From configuration mode in the CLI, enter the following command:

```
user@host# delete system scripts commit filename.xml
```

2. Commit the configuration:

```
user@host# commit
```

```
commit complete
```

To deactivate a commit script:

1. From configuration mode in the CLI, enter the following command:

```
user@host# deactivate system scripts commit filename.xml
```

2. Commit the configuration:

```
user@host# commit
```

```
commit complete
```



NOTE: You can later reactivate the commit script using the activate system scripts commit *filename.xml* command.

Automating Network Management and Troubleshooting with Operation Scripts

Operation scripts are scripts that you write to automate network management and troubleshooting tasks. They can perform any function available through JUNOScript remote procedure calls (RPCs).

This section contains the following topics:

- Operation Script Overview on page 138
- Enabling Operation Scripts on page 139
- Executing Operation Scripts on page 139
- Disabling Operation Scripts on page 140

Operation Script Overview

You can execute operation scripts from the JUNOS CLI or from within an event policy. For information about event policies, see “Running Self-Diagnostics with Event Policies” on page 140.

Operation scripts allow you to perform various actions, including the following:

- Automatically diagnose and fix problems in your network by building and running an operational mode command, receiving the command output, inspecting the output, and determining the next appropriate action. This process can be repeated until the source of the problem is determined and reported to the CLI.
- Monitor the overall status of the device by creating a general operation script that periodically checks network warning parameters, such as high CPU usage. The general operation script can be overridden by user-defined scripts.
- Customize the output of CLI operational mode commands using **printf** statements.
- If there is a known problem in JUNOS Software, an operation script can ensure your device is configured to avoid or work around the problem.
- Change your device's configuration in response to a problem.

The scripting language you use for writing operation scripts is Extensible Stylesheet Language Transformations (XSLT). XSLT operation scripts are based on JUNOScript Extensible Markup Language (XML).

Enabling Operation Scripts

To enable operation scripts:

1. Write an operation script.

For information about writing operation scripts, see the *JUNOS Configuration and Diagnostic Automation Guide*.

2. Copy the script to the `/var/db/scripts/op` directory.

Only users with superuser privileges can access and edit files in the `/var/db/scripts/op` directory.

3. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
4. Perform the configuration tasks described in Table 109 on page 139.
5. If you are finished configuring the network, commit the configuration.

Table 109: Enabling Operation Scripts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Op level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Scripts, click Configure or Edit. 4. Next to Op, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system scripts op
Enable the operation script file—for example, <code>op-script.xml</code> .	<ol style="list-style-type: none"> 1. Next to File, click Add new entry. 2. In the Name box, type <code>op-script.xml</code>. 3. Click OK. 	Set the script file name: set file op-script.xml

Executing Operation Scripts

You can execute the enabled operation scripts from the CLI or from within an event policy. For information about event policy, see “Running Self-Diagnostics with Event Policies” on page 140.

This section describes how you can execute operation scripts from the command line.

To execute an operation script from the CLI:

1. Enter configuration mode in the CLI.
2. Execute the script with the following command:

```
user@host# op filename.xml
```

Disabling Operation Scripts

If you do not want an operation script to run, you can disable it by deleting or deactivating it in the configuration. Deleting an operation script permanently removes it from the configuration. To run the script later, you must reenable the script as described in “Enabling Operation Scripts” on page 139. Deactivating an operation script disables the script until you activate it later.

To delete an operation script, do the following:

1. From configuration mode in the CLI, enter the following command:

```
user@host# delete system scripts op filename.xml
```

2. Commit the configuration:

```
user@host# commit
```

```
commit complete
```

To deactivate an operation script:

1. From configuration mode in the CLI, enter the following command:

```
user@host# deactivate system scripts op filename.xml
```

2. Commit the configuration:

```
user@host# commit
```

```
commit complete
```



NOTE: You can later reactivate the operation script using the `activate system scripts op filename.xml` command.

Running Self-Diagnostics with Event Policies

To diagnose a fault or error condition on a routing platform, you need relevant information about the state of the platform. You can derive state information from event notifications. Event notifications are system log messages and Simple Network Management Protocol (SNMP) traps.

Timely diagnosis and intervention can correct error conditions and keep the routing platform in operation. Event policies allow you to automatically initiate self-diagnostic

actions when specific events occur. These actions can either help you diagnose a fault or take corrective action.

This section contains the following topics:

- Event Policy Overview on page 141
- Configuring Event Policies on page 141

Event Policy Overview

In response to events, event policies can execute the following actions:

- Ignore the event—Do not generate a system log message for this event and do not process any further policy instructions for this event.
- Raise a trap—Initiate an SNMP trap to notify SNMP trap-based applications when the event occurs.
- Upload a file—Upload a file to a specified destination. You can specify a transfer delay, so that, on receipt of an event, the upload process begins after the configured transfer delay. For example, a transfer delay can ensure that a core file has been completely generated before being uploaded.
- Execute CLI operational mode commands—Execute commands when an event occurs. The output of these commands is stored in a file, which is then uploaded to a specified URL.
- Execute operation scripts—Execute operation scripts when an event occurs. The output of the operation scripts is stored in a file, which is then uploaded to a specified URL. For information about operation scripts, see “Automating Network Management and Troubleshooting with Operation Scripts” on page 138.

To view a list of the events that can be referenced in an event policy, issue the **help syslog ?** command:

```
user@host> help syslog ?
Possible completions:
<syslog-tag>          System log tag
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 record size
...
```

For information about these events, see the *JUNOS System Log Messages Reference*.

Configuring Event Policies

To configure event policies:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 110 on page 142.
3. If you are finished configuring the network, commit the configuration.

Table 110: Configuring Event Policies

Task	J-Web Configuration Editor	CLI Configuration Editor
Configuring Destination for Uploading Files for Analysis		
Navigate to the Destinations level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Event options, click Configure or Edit. 3. Next to Destinations, click Add new entry. 	From the [edit] hierarchy level, enter edit event-options destinations
Enter the destination name—for example, bsd2 . You can reference the destination in an event policy.	In the Destination name box, type bsd2 .	Set the destination name, the archive site location, and the password for accessing the archive site: set bsd2 archive-sites ftp://ftp.robot.net/event_analyze password eventadmin
Configure the archive site—for example, ftp://ftp.robot.net/event_analyze —where you want the output of commands executed by the event policy to be uploaded in a file for analysis, and the password—for example, eventadmin —for accessing the archive site.	<ol style="list-style-type: none"> 1. Next to Archive sites, click Add new entry. 2. In the Url box, type ftp://ftp.robot.net/event_analyze. 3. In the Password box, type eventadmin. 4. Click OK. 	
<p>NOTE: You can specify the archive site as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (SCP)-style remote file specification. URLs of the type file:// are also supported.</p> <p>NOTE: When you specify the archive site, do not add a slash (/) to the end of the URL. For example, do not specify the archive site as ftp://ftp.robot.net/event_analyze/.</p>		
Configuring Event Policy		
Navigate to the Policy level in the configuration hierarchy, and enter the policy name—for example, event1 .	<ol style="list-style-type: none"> 1. On the main Configuration page next to Event options, click Configure or Edit. 2. Next to Policy, click Add new entry. 3. In the Policy name box, type event1. 	From the [edit] hierarchy level, enter edit event-options policy event1
Configure the event name—for example, SNMP_TRAP_LINK_DOWN . The SNMP_TRAP_LINK_DOWN event occurs when an interface that is monitored by SNMP becomes unavailable.	<ol style="list-style-type: none"> 1. Next to Events, click Add new entry. 2. In the Event box, type SNMP_TRAP_LINK_DOWN. 3. Click OK. 	Set the event name: set events SNMP_TRAP_LINK_DOWN

Table 110: Configuring Event Policies (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Flag the event to initiate an SNMP trap when it generates a system log message.	<ol style="list-style-type: none"> Next to Then, click Configure. Select the Raise trap checkbox. Click OK. 	<p>Enter</p> <p>set then</p> <p>set raise-trap</p>
<p>Define the action to be taken when the configured event occurs.</p> <p>For example, configure the services router to do the following when the SNMP_TRAP_LINK_DOWN event occurs for the t1-3/0/0 interface:</p> <ol style="list-style-type: none"> Execute the show interfaces t1-3/0/0 and show configuration interfaces t1-3/0/0 commands. Upload the output of the show commands in a text file named config.txt to a server named bsd2. <p>NOTE: Do not include spaces, the slash, or the percent sign (%) in the filename.</p>	<ol style="list-style-type: none"> Next to Attributes match, click Add new entry. In the Condition list, select matches. In the From event attribute box, type SNMP_TRAP_LINK_DOWN.interface-name. In the To event attribute value box, type t1-3/0/0. Click OK. Next to Then, click Configure. Next to Execute commands, click Configure. In the Destination box, type bsd2. In the Output filename box, type config.txt. From the Output format list, select text. Next to Commands, click Add new entry. In the Command box, type show interfaces t1-3/0/0. Click OK. Next to Commands, click Add new entry. In the Command box, type show configuration interfaces t1-3/0/0. Click OK. 	<ol style="list-style-type: none"> Set the condition to execute the event policy only when the SNMP_TRAP_LINK_DOWN event occurs for the t1-3/0/0 interface: <p>set attributes-match SNMP_TRAP_LINK_DOWN.interface-name equals t1-3/0/0</p> Enter <p>edit then execute-commands</p> Set the commands to be executed when the configured event occurs: <p>set commands show interfaces t1-3/0/0</p> <p>set commands show configuration interfaces t1-3/0/0</p> Set the name and format of the file in which the output of the executed commands is to be uploaded to a destination server: <p>set output-filename config.txt output-format text</p> Set the name of the server to which the file containing the command output is to be uploaded: <p>set destination bsd2</p>

Part 3

Monitoring the Device

- Monitoring the Device and Routing Operations on page 147
- Monitoring Events and Managing System Log Files on page 229
- Configuring and Monitoring Alarms on page 239

Chapter 13

Monitoring the Device and Routing Operations

For information about which features you can monitor on your device, see the support information available at the beginning of this guide, the *JUNOS Software Interfaces and Routing Configuration Guide*, and the *JUNOS Software Security Configuration Guide*.

This chapter contains the following topics.

- Monitoring Overview on page 147
- Monitoring Interfaces on page 149
- Monitoring Events and Alarms on page 150
- Monitoring the System on page 150
- Monitoring NAT on page 156
- Monitoring Security Features on page 158
- Monitoring ALGs on page 179
- Monitoring VPNs on page 190
- Monitoring Enhanced Switching on page 198
- Monitoring Routing Information on page 202
- Monitoring Class-of-Service Performance on page 208
- Monitoring MPLS Traffic Engineering Information on page 214
- Monitoring PPPoE on page 219
- Monitoring PPP on page 222
- Monitoring the WAN Acceleration Interface on page 223
- Monitoring Services on page 223

Monitoring Overview

JUNOS Software 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 interface and CLI operational tools, you must have the appropriate access privileges. For more information about configuring access privilege levels, see “Adding New Users” on page 51 and the *JUNOS System Basics Configuration Guide*.)

You can use the J-Web Monitor and Manage options to monitor a device. J-Web results are displayed 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 complete descriptions of CLI operational mode commands, see the *JUNOS Software CLI Reference*, the *JUNOS System Basics and Services Command Reference*, the *JUNOS Interfaces Command Reference*, and the *JUNOS Routing Protocols and Policies Command Reference*.)

This section contains the following topics:

- Monitoring Terms on page 148
- Filtering Command Output on page 148

Monitoring Terms

Before monitoring your device, become familiar with the terms defined in Table 111 on page 148.

Table 111: Monitoring Terms

Term	Definition
autonomous system (AS)	Network of nodes that route packets based on a shared map of the network topology stored in their local databases.
Internet Control Message Protocol (ICMP)	TCP/IP protocol used to send error and information messages.
routing table	Database of routes learned from one or more protocols.

Filtering Command Output

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 is displayed on the screen. To limit the display to only those lines of the configuration that contain **address**, issue 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 --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

```

You can specify complex expressions as an option for the **match** and **except** filters. For more information about command output filtering and creating match expressions, see the *JUNOS CLI User Guide*.



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. See the *JUNOS CLI User Guide*.

Monitoring Interfaces

To view general information about all device physical and logical interfaces, select **Monitor > Interfaces** in the J-Web user interface.

Alternatively, you can enter the following **show** commands in the CLI editor to view interface status and traffic statistics:

- `show interfaces terse`
- `show interfaces detail`
- `show interfaces extensive`
- `show interfaces interface-name`

The J-Web Interfaces page displays the following details about each device interface:

- **Port**—Indicates the interface name. (For information about interface naming conventions, see the *JUNOS Software Interfaces and Routing Configuration Guide*.)
- **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).
- **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.

Monitoring Events and Alarms

For information about monitoring alarms, see “Checking Active Alarms” on page 247.

For information about viewing system events, see “Monitoring System Log Messages with the J-Web Event Viewer” on page 236.

Monitoring the System

The system properties include everything from the name and IP address of the device to the resource usage on the Routing Engine.

This topic contains:

- Monitoring System Properties (J Series) on page 150
- Monitoring System Properties (SRX Series) on page 151
- Monitoring Chassis Information on page 153
- Monitoring Process Details on page 156

Monitoring System Properties (J Series)

To view the system properties on a J Series device, select **Monitor > System View > System Information** in the J-Web interface.

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**

The System Information page displays the following types of information:

- **General**—The General tab of the System Information page displays the device's serial number, current software version, hostname, IP address, loopback address, domain name server, and time zone.



NOTE: The hostname that is displayed on this page is defined using the **set system hostname** command in the CLI editor. The time zone is defined using the **set system time-zone *time-zone*** command.

- **Time**—The 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**—The 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. For more information about monitoring memory usage, see “Monitoring Process Details” on page 156.
- **Logged-In User Details**—The 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**—The Active User Count field displays the number of users currently signed into the device.

Monitoring System Properties (SRX Series)

To view the system properties on an SRX Series device, select **Dashboard** in the J-Web interface.

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`

The Dashboard page displays the following types of information:

- Chassis View (Displayed by default)—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 on 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 Configure > Interfaces page for the selected port.
- Monitor Port: *Port-name*—Links to the Monitor > Interfaces page for the selected port.
- System Identification (Displayed by default)—Displays the device's serial number, hostname, current software version, the amount of time since the device was last booted, and the system's time.



NOTE: The hostname that is displayed on this page is defined using the `set system hostname` command in the CLI editor. The time zone is defined using the `set system time-zone time-zone` command.

- Resource Utilization (Displayed by default)—Displays the CPU, memory, and storage usage in graph bars.
- Security Resources (Displayed by default)—Displays the current number of sessions running on the device, firewall/VPN policies, and IPsec VPNs security resources details. Click the resource to redirect to details on the Monitor page.
- System Alarms (Hidden by default)—Indicates a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified.
- Login Sessions (Hidden by default)—Displays the log files, temporary files, crash files, and database file details.
- Chassis Status (Hidden by default)—Displays the chassis status report in detail.
- Storage Usage (Hidden by default)—Displays the storage usage report in detail.

- File Usage (Hidden by default)—Displays the file usage of log files, temporary files, crash (core) files, and database files.
- Message Logs (Always displayed)—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 is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Internet Explorer also causes the Chassis View to be displayed.

To control the information that is displayed in 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) From the Automatically Refresh Data list, specify how often you want the data on the page to be refreshed.
4. Click **OK** to save the configuration or **Cancel** to clear it.
5. (Optional) On the Dashboard page, minimize, maximize, or drag the individual information panes to customize the page display.

Monitoring Chassis Information

The chassis properties include the status of hardware components on the device. To view these chassis properties, select **Monitor > System View > Chassis Information** in the J-Web interface.

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`



CAUTION: Do not install a combination of 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. For more information, see the *J Series Services Routers Hardware Guide*.

The Chassis Information page displays the following types of information:

- **Routing Engine Details**—This section of the page includes the following tabs:
 - **Master**—The 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**—The Power tab displays the names of the device's power supply units and their statuses.
 - **Fan**—The 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**—The General tab displays the version number, part number, serial number, and description of the selected device component.
 - **Temperature**—The Temperature tab displays the temperature of the selected device component (if applicable).
 - **Resource**—The 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—The 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 are displayed, select a hardware component from the **Select component** list.

IOC to NPC Mapping

An Input/Output card (IOC) to Network Processing Card (NPC) mapping requires you to map one IOC to one NPC. However, you can map multiple IOCs to a single NPC. To balance the processing power in the NPC on the SRX3400 and SRX3600 Services Gateways, the chassis process (daemon) runs an algorithm that performs the mapping. It maps an IOC to an NPC that has the least amount of IOCs mapped to it. You can also use the command-line interface (CLI) to assign a specific IOC to a specific NPC. When you configure the mapping, the chassis process will first use your configuration, then apply the least-number NPC algorithm for the rest of the IOCs.

You can configure the IOC to NPC mapping using the following example:

```
set chassis ioc-npc-connectivity {
  ioc slot-number npc (none | slot-number);
}
```

The set chassis ioc-npc-connectivity options are described in Table 112 on page 155:

Table 112: IOC to NPC Connectivity Options

Option	Description
<i>ioc slot-number</i>	Specify the IOC slot number. Range is 0 through 7 for SRX3400 devices and 0 through 12 for SRX3600 devices.
<i>npc slot-number</i>	Specify the NPC slot number. Range is 0 through 7 for SRX3400 devices and 0 through 12 for SRX3600 devices.
none	The chassis process maps the connection for the particular IOC.



NOTE: You must restart the chassis control after you commit the **set chassis ioc-npc-connectivity** CLI command.

Monitoring Process Details

The process details indicates the status of each of the individual processes running on the device. To view these details, select **Monitor > System View > Process Details** in the J-Web interface.

Alternatively, you can view chassis details by entering the following **show** commands in the CLI configuration editor:

- **show chassis routing-engine**
- **show system process**

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 individual 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.

Monitoring NAT

The J-Web interface provides information about Network Address Translation (NAT).

This section contains the following topics:

- [Monitoring Incoming Table Information on page 156](#)
- [Monitoring Source NAT Information on page 157](#)

Monitoring Incoming Table Information

To view Network Address Translation table information, select **Monitor > NAT > Incoming Table** in the J-Web interface, or enter the following CLI command:

```
show security nat incoming-table
```


Table 113 on page 157 summarizes key output fields in the incoming table display.

Table 113: Summary of Key Incoming Table Output Fields

Field	Values	Additional Information
Incoming Table Summary		
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.	
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 Source NAT Information

To view the source Network Address Translation (NAT) summary table and the details of the specified NAT source address pool information, select **Monitor > NAT > Source NAT** in the J-Web interface, or enter the following CLI commands:

- `show security nat source-nat summary`
- `show security nat source-nat pool pool-name`

Table 114 on page 157 summarizes key output fields in the source NAT display.

Table 114: Summary of Key Source NAT Output Fields

Field	Values	Additional Information
Source NAT Summary Table		
Pool Name	Name of the source pool.	
Address Low	Starting IP address of one address range in the source pool.	
Address High	Ending IP address of one address range in the source pool.	
Interface	Name of the interface on which the source pool is defined.	

Table 114: Summary of Key Source NAT Output Fields *(continued)*

Field	Values	Additional Information
PAT	Whether Port Address Translation (PAT) is enabled (Yes, or No).	
Source NAT Pool Specific Summary: <i>pool-name</i>		
Address	IP address in the source pool.	
Interface	Name of the interface on which the source pool is defined.	
Status	Status of the IP address: <ul style="list-style-type: none"> ■ Active—Denotes that the IP address is in use. This status applies only to source NAT without Port Address Translation (PAT). ■ Free—IP address is available for allocation. 	
Single Ports	Number of allocated single ports.	
Twin Ports	Number of allocated twin ports.	
PAT	Whether PAT is enabled (Yes or No).	

Monitoring Security Features

This topic contains the following instructions:

- Monitoring Policies on page 158
- Monitoring Screen Counters on page 162
- Monitoring IDP on page 164
- Monitoring Flow Session Statistics on page 166
- Monitoring IDP on page 174
- Monitoring Flow Gate Information on page 174
- Monitoring Firewall Authentication on page 175
- Monitoring 802.1x on page 179

Monitoring Policies

The security policies information is divided into multiple parts. To view summary information such as the names of the source and destination addresses of the policy, the name of a preconfigured or custom application defined for the policy, or actions taken on packets matching the policies, select **Monitor > Security > Policies** in the J-Web interface. To view policy-specific properties such as policy or session statistics, select the policy name on the Security Policies page.

Alternatively, enter the following CLI commands:

- show security policies
- show security policies *policy-name policy-name*

Table 115 on page 159 summarizes key output fields in the security policies information display.

Table 115: Summary of Key Security Policies Information Output Fields

Field	Values	Additional Information
Security Policies Information		
Default policy	<p>Actions the device takes on a packet that does not match any user-defined policy:</p> <ul style="list-style-type: none"> ■ permit-all—Permit all traffic that does not match a policy. ■ deny-all—Deny all traffic that does not match a policy. Packets are dropped. This is the default. 	
From Zone	Name of the source zone.	
To Zone	Name of the destination zone.	
Policy Name	Name of the policy.	
Source Address	Names of the source addresses for a policy. Address sets are resolved to their individual names. (In this case, only the names are given, not their IP address).	
Destination Address	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.	
Applications	Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.	

Table 115: Summary of Key Security Policies Information Output Fields (*continued*)

Field	Values	Additional Information
Action	<p>Action taken in regard to a packet that matches the policy's tuples, or match conditions. Actions include the following:</p> <ul style="list-style-type: none"> ■ permit ■ IPsec-VPN tunnel <i>vpn-name</i> ■ pair-policy <i>pair-policy-name</i> ■ source-nat pool <i>pool-name</i> ■ interface ■ pool-set <i>pool-set-name</i> ■ destination-nat <i>name</i> ■ firewall-authentication ■ pass-through ■ web-authentication ■ deny ■ reject ■ count ■ log 	
State	<p>Status of the policy:</p> <ul style="list-style-type: none"> ■ enabled—The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. ■ disabled—The policy cannot be used in the policy lookup process, and therefore it is not available for access control. 	
Security Policies: <i>policy-name</i>		
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.	
From Zone	Name of the source zone.	
To Zone	Name of the destination zone.	

Table 115: Summary of Key Security Policies Information Output Fields (*continued*)

Field	Values	Additional Information
Action Type	<p>Action taken in regard to a packet that matches the policy's tuples, or match criteria. Actions include the following:</p> <ul style="list-style-type: none"> ■ permit ■ IPsec-VPN tunnel <i>vpn-name</i> ■ pair-policy <i>pair-policy-name</i> ■ source-nat pool <i>pool-name</i> ■ interface ■ pool-set <i>pool-set-name</i> ■ destination-nat <i>name</i> ■ firewall-authentication ■ pass-through ■ web-authentication ■ deny ■ reject ■ count ■ log 	
State	<p>Status of the policy:</p> <ul style="list-style-type: none"> ■ enabled—The policy can be used in the policy lookup process, which determines access rights for a packet and the action taken in regard to it. ■ disabled—The policy cannot be used in the policy lookup process, and therefore it is not available for access control. 	
Source addresses	Names and corresponding IP addresses of the source addresses for a policy. Address sets are resolved to their individual address name-IP address pairs.	
Destination addresses	Name of the destination address (or address set) as it was entered in the destination zone's address book. A packet's destination address must match this value for the policy to apply to it.	
Applications	<p>Name of a preconfigured or custom application whose type the packet matches, as specified at configuration time.</p> <ul style="list-style-type: none"> ■ IP protocol—The IP protocol used by the application—for example, TCP, UDP, ICMP. ■ ALG—If an ALG is associated with the session, the name of the ALG. Otherwise, 0. ■ Inactivity timeout—Elapsed time without activity after which the application is terminated. ■ Source port range—The low-high source port range for the session application. ■ Destination port range—The low-high destination port range for the session application. 	

Table 115: Summary of Key Security Policies Information Output Fields (*continued*)

Field	Values	Additional Information
Session log	Indicates whether the at-create and at-close flags were set at configuration time to log session information.	
Scheduler name	Name of a preconfigured scheduler whose schedule determines when the policy is active (or inactive). The device can use an active policy to check an incoming packet to determine how to treat the packet.	
Policy Statistics	Policy statistics include the following: <ul style="list-style-type: none"> ■ Input bytes—The number of bytes presented for processing by the device. ■ Output bytes—The number of bytes actually processed by the device. ■ Input packets—The number of packets presented for processing by the device. ■ Output packets—The number of packets actually processed by the device. 	
Session Statistics	Session statistics include the following: <ul style="list-style-type: none"> ■ Session creations—The number of sessions created since system startup. ■ Active sessions—The number of sessions currently present because of access control lookups that used this policy. ■ Session deletions—The number of sessions deleted since system startup. 	
Policy lookups	Number of times the policy was accessed to check for a match.	

Monitoring Screen Counters

To view screen statistics for a specified security zone, select **Monitor > Security > Screen Counters** in the J-Web interface, or enter the following CLI command:

```
show security screen statistics zone zone-name
```

Table 116 on page 163 summarizes key output fields in the screen counters display.

Table 116: Summary of Key Screen Counters Output Fields

Field	Values	Additional Information
Zones		
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.
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.

Table 116: Summary of Key Screen Counters Output Fields *(continued)*

Field	Values	Additional Information
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.	
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 Software rejects further connection requests from that IP address.
IP Block Fragment	Number of IP block fragments.	

Monitoring IDP

IDP monitoring pages allow you to display detailed information about the IDP Status, Memory, Counters, Policy rulebase statistics and Attack table statistics

This topic contains:

- Monitoring IDP Status on page 165

Monitoring IDP Status

To view Intrusion Detection and Prevention (IDP) table information, select **Monitor > Security > IDP > Status** in the J-Web interface, or enter the following CLI command:

- `show security idp status`
- `show security idp memory`

Table 117 on page 165 summarizes key output fields in the IDP display.

Table 117: Summary of IDP Status Output Fields

Field	Values	Additional Information
IDP Status		
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.	
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 Session Statistics

The J-Web interface provides session statistics according to the session filter you select on the Flow Session Statistics page.

This section contains the following topics:

- Monitoring Flow Session Statistics Summary Information on page 166
- Monitoring Flow Information for All Sessions on page 167
- Monitoring Flow Information for Application Sessions on page 167
- Monitoring Flow Session Destination Port Information on page 168
- Monitoring Flow Session Destination Prefix Information on page 169
- Monitoring Flow Session Interface Information on page 169
- Monitoring Flow Session Protocol Information on page 170
- Monitoring Flow Session Resource Manager on page 170
- Monitoring Flow Session Identifier Session on page 171
- Monitoring Flow Session Source Port Information on page 173
- Monitoring Flow Session Source Prefix Information on page 173
- Monitoring Flow Session Tunnel Information on page 174

Monitoring Flow Session Statistics Summary Information

To view summary information about existing sessions, including types of sessions, active and failed sessions, and the maximum allowed number of sessions, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **summary** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session summary
```

Table 118 on page 166 summarizes key output fields in the flow session statistics display.

Table 118: Summary of Key Flow Session Statistics Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—summary (By default)		
Unicast-sessions	Total number of active unicast sessions.	
Multicast-sessions	Total number of active multicast sessions.	
Failed-sessions	Total number of failed sessions.	
Active-sessions	Total number of active sessions.	
Maximum-sessions	Maximum number of supported sessions.	

Monitoring Flow Information for All Sessions

To view information about all currently active security sessions on the device, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **all** from the Session Filter list and click **Show**. To view information about the incoming and outgoing source and destination addresses and the protocol and interface for a specific session, select the session ID on the Flow Session Statistics page.

Alternatively, enter the following CLI command:

```
show security flow session
```

Table 119 on page 167 summarizes key output fields in the flow all session display.

Table 119: Summary of Key Flow All Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—all		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
Flow Session Statistics: Session ID		
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Information for Application Sessions

To view information about each session of the specified application type, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **application** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session application application-name
```

Table 120 on page 168 summarizes key output fields in the flow session application display.

Table 120: Summary of Key Flow Application Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—application		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Destination Port Information

To view information about each session that uses the specified destination port, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **destination port** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session destination-port destination-port-number
```

Table 121 on page 168 summarizes key output fields in the flow session destination port display.

Table 121: Summary of Key Flow Destination Port Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—destination port		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Destination Prefix Information

To view information about each session that uses the specified destination prefix, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **destination prefix** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session destination-prefix destination-prefix-number
```

Table 122 on page 169 summarizes key output fields in the flow session destination prefix display.

Table 122: Summary of Key Flow Destination Prefix Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—destination prefix		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Interface Information

To view information about each session that uses the specified incoming or outgoing interface, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **interface** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session interface interface-name
```

Table 123 on page 169 summarizes key output fields in the flow session interface display.

Table 123: Summary of Key Flow Interface Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—interface		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	

Table 123: Summary of Key Flow Interface Session Information Output Fields (*continued*)

Field	Values	Additional Information
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Protocol Information

To view information about each session that uses the specified protocol, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **protocol** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session protocol protocol-name
```

Table 124 on page 170 summarizes key output fields in the flow session protocol display.

Table 124: Summary of Key Flow Protocol Session Information Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—protocol		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Resource Manager

To view information about sessions created by the resource manager, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **resource manager** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

show security flow session resource-manager

Table 125 on page 171 summarizes key output fields in the flow session resource manager display.

Table 125: Summary of Key Flow Resource Manager Session Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—resource manager		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
Resource information	Information about the session particular to the resource manager, including the name of the ALG, the group ID, and the resource ID.	
Flow Session Statistics: Session ID		
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Identifier Session

To view information about the session, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **session identifier** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

show security flow session session-identifier *session-identifier*

Table 126 on page 171 summarizes key output fields in the flow session identifier session display.

Table 126: Summary of Key Flow Session Identifier Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—session identifier		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Status	Session status.	
Flag	Internal flag depicting the state of the session, used for debugging purposes.	

Table 126: Summary of Key Flow Session Identifier Output Fields *(continued)*

Field	Values	Additional Information
Virtual system	Virtual system to which the session belongs.	
Policy name	Name and ID of the policy that the first packet of the session matched.	
Maximum timeout	Maximum session timeout.	
Current timeout	Remaining time for the session unless traffic exists in the session.	
Start time	Time when the session was created, offset from the system start time.	
Duration	Length of time for which the session is active.	
In	For the input flow: <ul style="list-style-type: none"> ■ Source and destination addresses and protocol tuple for the input flow. ■ Interface: Input flow interface. ■ Session token: Internal token derived from the virtual routing instance. ■ Flag: Internal debugging flags. ■ Route: Internal next hop of the route to be used by the flow. ■ Gateway: Next-hop gateway of the flow. ■ Tunnel: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero). ■ Port Sequence, FIN sequence, FIN state, Cookie: Internal TCP state tracking information. 	
Out	For the reverse flow: <ul style="list-style-type: none"> ■ Source and destination addresses and protocol tuple for the input flow. ■ Interface: Input flow interface. ■ Session token: Internal token derived from the virtual routing instance. ■ Flag: Internal debugging flags. ■ Route: Internal next hop of the route to be used by the flow. ■ Gateway: Next-hop gateway of the flow. ■ Tunnel: If the flow is going into a tunnel, the tunnel ID. Otherwise, 0 (zero). ■ Port Sequence, FIN sequence, FIN state, Cookie: Internal TCP state tracking information. 	

Monitoring Flow Session Source Port Information

To view information about each session that uses the specified source port, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **source port** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session source-port source-port-number
```

Table 127 on page 173 summarizes key output fields in the flow session source port display.

Table 127: Summary of Key Flow Source Port Session Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—source port		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Source Prefix Information

To view information about each session that uses the specified source prefix, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **source prefix** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session source-prefix source-prefix-number
```

Table 128 on page 173 summarizes key output fields in the flow session source prefix display.

Table 128: Summary of Key Flow Source Prefix Session Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—source prefix		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	

Table 128: Summary of Key Flow Source Prefix Session Output Fields *(continued)*

Field	Values	Additional Information
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	
Out	Reverse flow (source and destination IP addresses, application protocol, and interface).	

Monitoring Flow Session Tunnel Information

To view information about all tunnel session, select **Monitor > Security > Flow Session Statistics** in the J-Web interface. Then select **tunnel** from the Session Filter list and click **Show**. Alternatively, enter the following CLI command:

```
show security flow session tunnel
```

Table 129 on page 174 summarizes key output fields in the flow session tunnel display.

Table 129: Summary of Key Flow Tunnel Session Output Fields

Field	Values	Additional Information
Flow Session Statistics: session filter—tunnel		
Session ID	Number that identifies the session. Use this ID to get more information about the session.	
Policy name	Policy that permitted the traffic.	
Timeout	Idle timeout after which the session expires.	
In	Incoming flow (source and destination IP addresses, application protocol, and interface).	

Monitoring IDP

For information about monitoring Intrusion Detection and Prevention features, see the *JUNOS Software Security Configuration Guide*.

Monitoring Flow Gate Information

To view information about temporary openings known as pinholes or gates in the security firewall, select **Monitor > Security > Flow Gate Information** in the J-Web interface, or enter the following CLI command:

show security flow gate

Table 130 on page 175 summarizes key output fields in the flow gate display.

Table 130: Summary of Key Flow Gate Output Fields

Field	Values	Additional Information
Flow Gate Information		
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"> ■ Source address and port ■ Destination address and port 	
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

The J-Web interface provides information about user authentications and history of authentications.

This section contains the following topics:

- Monitoring Firewall Authentication Table on page 175
- Monitoring Firewall Authentication History on page 177

Monitoring Firewall Authentication Table

The firewall authentication user information is divided into multiple parts. To view information about authentication table, select **Monitor > Security > Firewall Authentication > Authentication Table** in the J-Web 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 commands:

- show security firewall-authentication users
- show security firewall-authentication users address *ip-address*
- show security firewall-authentication users identifier *identifier*

Table 131 on page 176 summarizes key output fields in firewall authentication table display.

Table 131: Summary of Key Firewall Authentication Table Output Fields

Field	Values	Additional Information
Firewall authentication users		
Total users in table	Number of users in the authentication table.	
Authentication table		
ID	Authentication identification number.	
Source Ip	IP address of the authentication source.	
Age	Idle timeout for the user.	
Status	Status of authentication (success or failure).	
user	Name of the user.	
Detailed report per ID selected: ID		
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.	
Detailed report per Source Ip selected		
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.	

Table 131: Summary of Key Firewall Authentication Table Output Fields (*continued*)

Field	Values	Additional Information
Age	Idle timeout for the user.	
Status	Status of authentication (success or failure).	
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

The firewall authentication history information is divided into multiple parts. To view information about the authentication history, select **Monitor > Security > Firewall Authentication > Authentication History** in the J-Web 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 132 on page 177 summarizes key output fields in firewall authentication history display.

Table 132: Summary of Key Firewall Authentication History Output Fields

Field	Values	Additional Information
History of Firewall Authentication Data		
Total authentications	Number of authentication.	
History Table		
ID	Identification number.	
Source Ip	IP address of the authentication source.	

Table 132: 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 (success or failure).	
User	Name of the user.	
Detail history of selected Id: ID		
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.	
Detail history of selected Source Ip:Source Ip		
User	Name of the user.	
Start Date	Authentication date.	
Start Time	Authentication time.	
Duration	Authentication duration.	
Status	Status of authentication (success or failure).	
Profile	Name of the profile.	
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.	

Table 132: Summary of Key Firewall Authentication History Output Fields (*continued*)

Field	Values	Additional Information
Bytes received by this user	Number of packets in bytes received by this user.	
Client-groups	Name of the client group.	

Monitoring 802.1x

To view information about 802.1X properties, select **Monitor > Security > 802.1x** in the J-Web interface or enter the following CLI commands:

- show dot1x interfaces *interface-name*
- show dot1x authentication-failed-users

Table 133 on page 179 summarizes the Dot1X output fields.

Table 133: 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.	
Authenticated Users Summary		
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.	
Authentication Failed Users Summary		
MAC Address	MAC address of the authentication-failed host.	
User Name	Name of the authentication-failed user.	

Monitoring ALGs

The J-Web interface provides detailed information about the SIP, H.323, MGCP, and SCCP ALGs.

This section contains the following topics:

- Monitoring SIP ALG Information on page 180
- Monitoring H.323 ALG Information on page 184
- Monitoring MGCP ALG Information on page 185
- Monitoring SCCP ALG Information on page 188

Monitoring SIP ALG Information

The J-Web interface provides information for SIP ALG calls, counters, rates, and transactions.

This section contains the following topics:

- Monitoring SIP ALG Calls on page 180
- Monitoring SIP ALG Counters on page 181
- Monitoring SIP ALG Rate Information on page 183
- Monitoring SIP ALG Transactions on page 183

Monitoring SIP ALG Calls

To view information about SIP ALG calls, select **Monitor > ALGs > SIP > Calls** in the J-Web interface. To view detailed information, select the Call Leg on the SIP calls page.

Alternatively, enter the following CLI command:

```
show security alg sip calls detail
```

Table 134 on page 180 summarizes key output fields in the SIP calls display.

Table 134: Summary of Key SIP Calls Output Fields

Field	Values	Additional Information
SIP Calls Information		
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

To view SIP ALG counters information, select **Monitor > ALGs > SIP > Count** in the J-Web interface, or enter the following CLI command:

```
show security alg sip counters
```

Table 135 on page 181 summarizes key output fields in the SIP counters display.

Table 135: Summary of Key SIP Counters Output Fields

Field	Values	Additional Information
SIP Counters Information		
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 135: 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.
SIP Error Counters		
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

To view SIP ALG rate information, select **Monitor > ALGs > SIP > Rate** in the J-Web interface, or enter the following CLI command:

```
show security alg sip rate
```

Table 136 on page 183 summarizes key output fields in the SIP rate display.

Table 136: Summary of Key SIP Rate Output Fields

Field	Values	Additional Information
SIP Rate Information		
CPU ticks per microseconds is	SIP ALG CPU ticks per microsecond.	
Time taken for the last message in microseconds is	Time, in microseconds, that the last SIP ALG message needed to transit the network.	
Number of messages in 10 minutes	Total number of SIP ALG messages transiting the network in 10 minutes.	
Time taken by the messages in 10 minutes	Total time, in microseconds, during an interval of less than 10 minutes for the specified number of SIP ALG messages to transit the network.	
Rate	Number of SIP ALG messages per second transiting the network.	

Monitoring SIP ALG Transactions

To view information about SIP ALG transactions, select **Monitor > ALGs > SIP > Transactions** in the J-Web interface, or enter the following CLI command:

```
show security alg sip transactions
```

Table 137 on page 184 summarizes key output fields in the SIP transactions display.

Table 137: Summary of Key SIP Transactions Output Fields

Field	Values	Additional Information
SIP Transactions Information		
Transaction Name	<ul style="list-style-type: none"> ■ UAS—SIP ALG User Agent server transaction name. ■ UAC—SIP ALG User Agent client transaction name. 	
Method	<p>The method to be performed on the resource. Possible methods:</p> <ul style="list-style-type: none"> ■ INVITE—Initiate call ■ ACK—Confirm final response ■ BYE—Terminate and transfer call ■ CANCEL—Cancel searches and “ringing” ■ OPTIONS—Features support by the other side ■ REGISTER—Register with location service 	

Monitoring H.323 ALG Information

To view the H.323 ALG counters information, select **Monitor > ALGs > H323** in the J-Web interface, or enter the following CLI command:

```
show security alg h323 counters
```

Table 138 on page 184 summarizes key output fields in the H.323 counters display.

Table 138: Summary of Key H.323 Counters Output Fields

Field	Values	Additional Information
H.323 Counters Information		
Packets received	Number of H.323 ALG packets received.	
Packets dropped	Number of H.323 ALG packets dropped.	
RAS message received	Number of incoming RAS (Endpoint Registration, Admission, and Status) messages per second per gatekeeper received and processed.	
Q.931 message received	Counter for Q.931 message received.	
H.245 message received	Counter for H.245 message received.	
Number of calls	Total number of H.323 ALG calls.	

Table 138: Summary of Key H.323 Counters Output Fields (*continued*)

Field	Values	Additional Information
Number of active calls	Number of active H.323 ALG calls.	This counter displays the number of call legs and may 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.
H.323 Error Counters		
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.	

Monitoring MGCP ALG Information

The J-Web interface provides information for MGCP ALG calls, counters, and endpoints.

This section contains the following topics:

- Monitoring MGCP ALG Calls on page 185
- Monitoring MGCP ALG Counters on page 186
- Monitoring MGCP ALG Endpoints on page 187

Monitoring MGCP ALG Calls

To view information about MGCP ALG calls, select **Monitor > ALGs > MGCP > Calls** in the J-Web interface. To view detailed information, select the endpoint on the MGCP calls page.

Alternatively, enter the following CLI command:

```
show security alg mgcp calls
```

Table 139 on page 186 summarizes key output fields in the MGCP calls display.

Table 139: Summary of Key MGCP Calls Output Fields

Field	Values	Additional Information
MGCP Calls Information		
Endpoint@GW	Endpoint name.	
Zone	<div><div>■</div>trust—Trust zone.</div> <div><div>■</div>untrust—Untrust zone.</div>	
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.	
Calls Details: Endpoint		
Local SDP	IP address of the MGCP ALG local call owner, as per the Session Description Protocol (SDP).	
Remote SDP	Remote IP address of the MGCP ALG remote call owner, as per the Session Description Protocol (SDP).	

Monitoring MGCP ALG Counters

To view MGCP ALG counters information, select **Monitor > ALGs > MGCP > Counters** in the J-Web interface, or enter the following CLI command:

```
show security alg mgcp counters
```

Table 140 on page 186 summarizes key output fields in the MGCP counters display.

Table 140: Summary of Key MGCP Counters Output Fields

Field	Values	Additional Information
MGCP Counters Information		
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.	

Table 140: Summary of Key MGCP Counters Output Fields (continued)

Field	Values	Additional Information
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.	
Error Counters		
Unknown-method	MGCP ALG unknown method errors.	
Decoding error	MGCP ALG decoding errors.	
Transaction error	MGCP ALG transaction errors.	
Call error	MGCP ALG counter errors.	
Connection error	MGCP ALG connection errors.	
Connection flood drop	MGCP ALG connection flood drop errors.	
Message flood drop	MGCP ALG message flood drop error.	
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

To view information about MGCP ALG endpoints, select **Monitor > ALGs > MGCP > Endpoints** in the J-Web interface. To view detailed information, select the gateway on the MGCP endpoints page.

Alternatively, enter the following CLI command:

```
show security alg mgcp endpoints
```

Table 141 on page 187 summarizes key output fields in the MGCP endpoints display.

Table 141: Summary of Key MGCP Endpoints Output Fields

Field	Values	Additional Information
MGCP Endpoints		
Gateway	IP address of the gateway.	

Table 141: Summary of Key MGCP Endpoints Output Fields *(continued)*

Field	Values	Additional Information
Zone	<ul style="list-style-type: none"> ■ trust—Trust zone. ■ untrust—Untrust zone. 	
IP	IP address.	
Endpoints: Gateway name		
Endpoint	Endpoint name.	
Transaction #	Transaction identifier.	
Call #	Call identifier.	
Notified Entity	The certificate authority (CA) currently controlling the gateway.	

Monitoring SCCP ALG Information

The J-Web interface provides information for SCCP ALG calls, and counters.

This section contains the following topics:

- Monitoring SCCP ALG Calls on page 188
- Monitoring SCCP ALG Counters on page 189

Monitoring SCCP ALG Calls

To view information about SCCP ALG calls, select **Monitor > ALGs > SCCP > Calls** in the J-Web interface. To view detailed information, select the client IP address on the SCCP calls page.

Alternatively, enter the following CLI show command:

```
show security alg sccp calls
```

Table 142 on page 188 summarizes key output fields in the SCCP calls display.

Table 142: Summary of Key SCCP Calls Output Fields

Field	Values	Additional Information
SCCP Calls Information		
Client IP	IP address of the client.	
Zone	Client zone identifier.	
Call Manager	IP address of the call manager.	

Table 142: Summary of Key SCCP Calls Output Fields *(continued)*

Field	Values	Additional Information
Conference ID	Conference call identifier.	
RM Group	Resource manager group identifier.	

Monitoring SCCP ALG Counters

To view SCCP ALG counters information, select **Monitor > ALGs > SCCP > Count** in the J-Web interface, or enter the following CLI command:

```
show security alg sccp counters
```

Table 143 on page 189 summarizes key output fields in the SCCP counters display.

Table 143: Summary of Key SCCP Counters Output Fields

Field	Values	Additional Information
SCCP Counters Information		
Clients currently registered	Number of SCCP ALG clients currently registered.	
Active calls	Number of active SCCP ALG calls.	
Total calls	Total number of SCCP ALG calls.	
Packets received	Number of SCCP ALG packets received.	
PDUs processed	Number of SCCP ALG protocol data units (PDUs) processed.	
Current call rate	Number of calls per second.	
Error counters		
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.	

Table 143: Summary of Key SCCP Counters Output Fields *(continued)*

Field	Values	Additional Information
Policy lookup errors	Number of packets dropped because of a failed policy lookup.	
Unknown PDUs	Number of unknown protocol data units (PDUs).	
Maximum calls exceed	Number of times the maximum SCCP calls limit was exceeded.	
Maximum call rate exceed	Number of times the maximum SCCP call rate exceeded.	
Initialization errors	Number of initialization errors.	
Internal errors	Number of internal errors.	
Unsupported feature	Number of unsupported feature errors.	
Non specific error	Number of nonspecific errors.	

Monitoring VPNs

The J-Web interface provides information about IKE and IPsec security associations (SAs).

This section contains the following topics:

- Monitoring IKE Gateway Information on page 190
- Monitoring IPsec VPN Information on page 194

Monitoring IKE Gateway Information

To view information about IKE security associations (SAs), select **Monitor > IPsec VPN > IKE Gateway** in the J-Web 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 144 on page 191 summarizes key output fields in the IKE gateway display.

Table 144: Summary of Key IKE SA Information Output Fields

Field	Values	Additional Information
IKE Security Associations		
IKE SA Index	Index number of an SA.	This number is an internally generated number you can use to display information about a single SA.
Remote Address	IP address of the destination peer with which the local peer communicates.	
State	State of the IKE security associations: <ul style="list-style-type: none"> ■ DOWN—SA has not been negotiated with the peer. ■ UP—SA has been negotiated with the peer. 	
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.	
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.	A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.
Mode	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are <ul style="list-style-type: none"> ■ 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. ■ 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. 	
IKE Security Association (SA) Index		
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.	

Table 144: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
State	State of the IKE security associations: <ul style="list-style-type: none"> ■ DOWN—SA has not been negotiated with the peer. ■ UP—SA has been negotiated with the peer. 	
Initiator cookie	Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.	
Responder cookie	Random number generated by the remote node and sent back to the initiator as a verification that the packets were received.	A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.
Exchange Type	Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between themselves. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are <ul style="list-style-type: none"> ■ 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. ■ 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. 	
Authentication Method	Path chosen for authentication.	
Local	Address of the local peer.	
Remote	Address of the remote peer.	
Lifetime	Number of seconds remaining until the IKE SA expires.	

Table 144: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
Algorithm	<p>IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:</p> <ul style="list-style-type: none"> ■ Authentication—Type of authentication algorithm used. <ul style="list-style-type: none"> ■ sha1—Secure Hash Algorithm 1 (SHA-1) authentication. ■ md5—MD5 authentication. ■ Encryption—Type of encryption algorithm used. <ul style="list-style-type: none"> ■ aes-256-cbc—Advanced Encryption Standard (AES) 256-bit encryption. ■ aes-192-cbc—Advanced Encryption Standard (AES) 192-bit encryption. ■ aes-128-cbc—Advanced Encryption Standard (AES) 128-bit encryption. ■ 3des-cbc—3 Data Encryption Standard (DES) encryption. ■ des-cbc—Data Encryption Standard (DES) encryption. ■ Pseudo random function—Cryptographically secure pseudorandom function family. 	
Traffic Statistics	<p>Traffic statistics include the following:</p> <ul style="list-style-type: none"> ■ Input bytes—The number of bytes presented for processing by the device. ■ Output bytes—The number of bytes actually processed by the device. ■ Input packets—The number of packets presented for processing by the device. ■ Output packets—The number of packets actually processed by the device. 	
IPsec security associations	<ul style="list-style-type: none"> ■ number created—The number of SAs created. ■ number deleted—The number of SAs deleted. 	
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.	

Table 144: Summary of Key IKE SA Information Output Fields (*continued*)

Field	Values	Additional Information
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 Information

To view information about IPsec security (SAs), select **Monitor > IPsec VPN > IPsec VPN** in the J-Web 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 145 on page 194 summarizes key output fields in the IPsec VPN display.

Table 145: Summary of Key IPsec VPN Information Output Fields

Field	Values	Additional Information
IPsec Security Associations		
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"> ■ An authentication algorithm used to authenticate exchanges between the peers. Options are <code>hmac-md5-95</code> or <code>hmac-sha1-96</code>. ■ An encryption algorithm used to encrypt data traffic. Options are <code>3des-cbc</code>, <code>aes-128-cbc</code>, <code>aes-192-cbc</code>, <code>aes-256-cbc</code>, or <code>des-cbc</code>. 	

Table 145: Summary of Key IPsec VPN Information Output Fields (continued)

Field	Values	Additional Information
SPI	Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.	
Life: sec/kb	The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.	
State	<p>State has two options, Installed and Not Installed.</p> <ul style="list-style-type: none"> ■ Installed—The security association is installed in the security association database. ■ Not Installed—The security association is not installed in the security association database. 	For transport mode, the value of State is always Installed .
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"> ■ Encrypted bytes—Total number of bytes encrypted by the local system across the IPsec tunnel. ■ Decrypted bytes—Total number of bytes decrypted by the local system across the IPsec tunnel. ■ Encrypted packets—Total number of packets encrypted by the local system across the IPsec tunnel. ■ Decrypted packets—Total number of packets decrypted by the local system across the IPsec tunnel. 	
AH Statistics	<p>Authentication Header (AH) statistics include the following:</p> <ul style="list-style-type: none"> ■ Input bytes—The number of bytes presented for processing by the device. ■ Output bytes—The number of bytes actually processed by the device. ■ Input packets—The number of packets presented for processing by the device. ■ Output packets—The number of packets actually processed by the device. 	

Table 145: Summary of Key IPsec VPN Information Output Fields *(continued)*

Field	Values	Additional Information
Errors	<p>Errors include the following</p> <ul style="list-style-type: none"> ■ AH authentication failures—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. ■ Replay errors—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window. ■ ESP authentication failures—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets. ■ ESP decryption failures—Total number of ESP decryption errors. ■ Bad headers—Total number of invalid headers detected. ■ Bad trailers—Total number of invalid trailers detected. 	
Details for IPsec SA Index: ID		
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— set or cleared .	
Policy name	Name of the applicable policy.	
Direction	Direction of the security association— inbound , or outbound .	
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.	

Table 145: Summary of Key IPsec VPN Information Output Fields *(continued)*

Field	Values	Additional Information
Mode	<p>Mode of the security association. Mode can be transport or tunnel.</p> <ul style="list-style-type: none"> ■ transport—Protects host-to-host connections. ■ tunnel—Protects connections between security gateways. 	
Type	<p>Type of the security association, either manual or dynamic.</p> <ul style="list-style-type: none"> ■ manual—Security parameters require no negotiation. They are static and are configured by the user. ■ dynamic—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode. 	
State	<p>State has two options, Installed, and Not Installed.</p> <ul style="list-style-type: none"> ■ Installed—The security association is installed in the security association database. ■ Not Installed—The security association is not installed in the security association database. 	For transport mode, the value of State is always Installed .
Protocol	<p>Protocol supported:</p> <ul style="list-style-type: none"> ■ Transport mode supports Encapsulation Security Protocol (ESP) and Authentication Header (AH). ■ Tunnel mode supports ESP and AH. <ul style="list-style-type: none"> ■ Authentication—Type of authentication used. ■ Encryption—Type of encryption used. 	

Table 145: Summary of Key IPsec VPN Information Output Fields *(continued)*

Field	Values	Additional Information
Authentication/ Encryption	<ul style="list-style-type: none"> ■ Authentication—Type of authentication algorithm used. <ul style="list-style-type: none"> ■ sha1—Secure Hash Algorithm 1 (SHA-1) authentication. ■ md5—MD5 authentication. ■ Encryption—Type of encryption algorithm used. <ul style="list-style-type: none"> ■ aes-256-cbc—Advanced Encryption Standard (AES) 256-bit encryption. ■ aes-192-cbc—Advanced Encryption Standard (AES) 192-bit encryption. ■ aes-128-cbc—Advanced Encryption Standard (AES) 128-bit encryption. ■ 3des-cbc—3 Data Encryption Standard (DES) encryption. ■ des-cbc—Data Encryption Standard (DES) encryption. 	
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"> ■ Expires in seconds—Number of seconds left until the SA expires. ■ Expires in kilobytes—Number of kilobytes left until the SA expires. 	Each lifetime of a security association has two display options, hard and soft , 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"> ■ Expires in seconds—Number of seconds left until the SA expires. ■ Expires in kilobytes—Number of kilobytes left until the SA expires. 	
Anti Replay Service	State of the service that prevents packets from being replayed. It can be Enabled or Disabled .	
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.

Monitoring Enhanced Switching

New Monitor pages for enhanced switching allow you to monitor the information and status about the following:

- Monitoring Ethernet Switching on page 199
- Monitoring Spanning Tree on page 200

- Monitoring IGMP Snooping on page 201
- Monitoring GVRP on page 201

Monitoring Ethernet Switching

To view information about the Ethernet Switching interface details, select **Monitor > Switching > Ethernet Switching** in the J-Web interface, or enter the following CLI command:

- `show ethernet-switching table`
- `show ethernet-switching mac-learning-log`

Table 146 on page 199 summarizes the Ethernet Switching output fields.

Table 146: 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"> ■ static—The MAC address is manually created. ■ learn—The MAC address is learned dynamically from a packet's source MAC address. ■ flood—The MAC address is unknown and flooded to all members. 	
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).	
VLAN-ID	The VLAN ID.	
MAC Address	The learned MAC address.	
Time	Timestamp when the MAC address was added or deleted from the log.	
State	Indicates the MAC address learned on the interface.	

Monitoring Spanning Tree

To view status and information about the spanning tree interface parameters, select **Monitor > Switching > Spanning Tree** in the J-Web interface or enter the following CLI commands:

- show spanning-tree interface
- show spanning-tree bridge

Table 147 on page 200 summarizes the Spanning Tree output fields.

Table 147: Summary of Spanning Tree Output Fields

Field	Values	Additional Information
Spanning Tree Bridge Parameters		
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.	
Maximum age	Maximum age of received bridge protocol data units (BPDUs).	
Number of topology changes	Total number of STP topology changes detected since the switch last booted.	
Interface List		
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.	

Monitoring IGMP Snooping

To view information about the IGMP snooping parameters, select **Monitor > Switching > IGMP-Snooping** in the J-Web interface, or enter the following CLI commands:

- `show igmp-snooping vlans`
- `show igmp-snooping route`

Table 148 on page 201 summarizes the IGMP Snooping output fields.

Table 148: Summary of IGMP Snooping Output Fields

Field	Values	Additional Information
VLAN	The VLAN for which IGMP snooping is enabled.	
Interfaces	Indicates the number of interfaces in the VLAN.	
Groups	Indicates the multicast groups learned by the VLAN.	
MRouters	Indicates the MRouters learned by the VLAN.	
Receivers	Specifies the multicast receiver.	
Group	Indicates the multicast groups learned by the VLAN.	
Next-Hop	The next hop assigned by the switch after performing the route lookup.	

Monitoring GVRP

To view information about global GVRP configuration, select **Monitor > Switching > GVRP** in the J-Web interface or enter the following CLI command:

`show gvrp`

Table 149 on page 201 summarizes the GVRP output fields.

Table 149: Summary of GVRP Output Fields

Field	Values	Additional Information
GVRP		

Table 149: Summary of GVRP Output Fields *(continued)*

Field	Values	Additional Information
Global GVRP Configuration	List of global GVRP configuration statistics such as: <ul style="list-style-type: none"> ■ GVRP status—Displays whether GVRP is enabled or disabled. ■ 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. 	
Interfaces	List of interface-based configuration statistics: <ul style="list-style-type: none"> ■ Interface Name—The interface on which GVRP is configured. ■ Protocol Status—Displays whether GVRP is enabled or disabled. 	

Monitoring Routing Information

The J-Web interface provides information about routing tables and routing protocols.

This section contains the following topics:

- Monitoring Route Information on page 202
- Monitoring RIP Routing Information on page 204
- Monitoring OSPF Routing Information on page 204
- Monitoring BGP Routing Information on page 206
- Monitoring DLSw Routing Information on page 207

Monitoring Route Information

To view information about the routes in a routing table, including destination, protocol, state, and parameter information, in the J-Web interface, select **Monitor > Routing > Route Information**, or enter the following CLI commands:

- `show route terse`
- `show route detail`

Table 150 on page 203 summarizes key output fields in the routing information display.

Table 150: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
<i>n</i> destinations	Number of destinations for which there are routes in the routing table.	
<i>n</i> routes	Number of routes in the routing table: <ul style="list-style-type: none"> ■ active—Number of routes that are active. ■ holddown—Number of routes that are in hold-down state (neither advertised nor updated) before being declared inactive. ■ hidden—Number of routes not used because of routing policies configured on the device. 	
Destination	Destination address of the route.	
Protocol/ Preference	Protocol from which the route was learned: Static , Direct , Local , or the name of a particular protocol. 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 Discard, 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 Discard attribute has been set.</p> <p>If a next hop is listed as Reject, 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 Local, the destination is an address on the host (either the loopback address or the Ethernet management port 0 address, for example).</p>
Age	How long the route has been known.	
State	Flags for this route.	There are many possible flags. For a complete description, see the <i>JUNOS Interfaces Command Reference</i> .
AS Path	AS path through which the route was learned. The letters of the AS path indicate the path origin: <ul style="list-style-type: none"> ■ I — IGP. ■ E — EGP. ■ ? — Incomplete. Typically, the AS path was aggregated. 	

Monitoring RIP Routing Information

To view RIP routing information, including a summary of RIP neighbors and statistics, select **Monitor > Routing > RIP Information**, or enter the following CLI commands:

- show rip statistics
- show rip neighbors

Table 151 on page 204 summarizes key output fields in the RIP routing display.

Table 151: Summary of Key RIP Routing Output Fields

Field	Values	Additional Information
RIP Statistics		
Rip info	Information about RIP on the specified interface, including UDP port number, hold-down interval (during which routes are neither advertised nor updated), and timeout interval.	
Logical interface	Name of the logical interface on which RIP is configured.	
Routes learned	Number of RIP routes learned on the logical interface.	
Routes advertised	Number of RIP routes advertised on the logical interface.	
RIP Neighbors		
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. The name is set in the CLI configuration editor, with the neighbor neighbor-name statement at the [edit protocols rip group group-name] level of the configuration hierarchy.
State	State of the RIP connection: Up or Dn (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.
In Met	Value of the incoming metric configured for the RIP neighbor.	

Monitoring OSPF Routing Information

To view OSPF routing information, including a summary of OSPF neighbors, interfaces, and statistics, select **Monitor > Routing > OSPF Information**, or enter the following CLI commands:

- show ospf neighbors
- show ospf interfaces
- show ospf statistics

Table 152 on page 205 summarizes key output fields in the OSPF routing display.

Table 152: Summary of Key OSPF Routing Output Fields

Field	Values	Additional Information
OSPF Neighbors		
Address	Address of the neighbor.	
Interface	Interface through which the neighbor is reachable.	
State	State of the neighbor: Attempt, Down, Exchange, ExStart, Full, Init, Loading, or 2way.	Generally, only the Down state, indicating a failed OSPF adjacency, and the Full 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	Router ID of the neighbor.	
Priority	Priority of the neighbor to become the designated router.	
Dead	Number of seconds until the neighbor becomes unreachable.	
OSPF Interfaces		
Interface	Name of the interface running OSPF.	
State	State of the interface: BDR, Down, DR, DRother, Loop, PtToPt, or Waiting.	The Down state, indicating that the interface is not functioning, and PtToPt 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	Address of the area's designated router.	
BDR ID	Address of the area's backup designated router.	
Nbrs	Number of neighbors on this interface.	
OSPF Statistics		
Packet Type	Type of OSPF packet.	
Total Sent/Total Received	Total number of packets sent and received.	

Table 152: Summary of Key OSPF Routing Output Fields *(continued)*

Field	Values	Additional Information
Last 5 seconds Sent/Last 5 seconds Received	Total number of packets sent and received in the last 5 seconds.	
Receive errors	Number and type of receive errors.	

Monitoring BGP Routing Information

To view BGP routing information, including a summary of BGP routing and neighbor information, select **Monitor > Routing > BGP Information**, or enter the following CLI commands:

- show bgp summary
- show bgp neighbor

Table 153 on page 206 summarizes key output fields in the BGP routing display.

Table 153: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Summary		
Groups	Number of BGP groups.	
Peers	Number of BGP peers.	
Down Peers	Number of unavailable BGP peers.	
Peer	Address of each BGP peer.	
InPkt	Number of packets received from the peer.	
OutPkt	Number of packets sent to the peer.	
Flaps	Number of times a BGP session has changed state from Down to Up.	A high number of flaps might indicate a problem with the interface on which the BGP session is enabled.
Last Up/Down	Last time that a session became available or unavailable, since the neighbor transitioned to or from the established state.	If the BGP session is unavailable, this time might be useful in determining when the problem occurred.

Table 153: Summary of Key BGP Routing Output Fields (*continued*)

Field	Values	Additional Information
State	<p>A multipurpose field that displays information about BGP peer sessions. The contents of this field depend upon whether a session is established.</p> <ul style="list-style-type: none"> ■ If a peer is not established, the field shows the state of the peer session: Active, Connect, or Idle. ■ If a BGP session is established, the field shows the number of active, received, and damped routes that are received from a neighbor. For example, 2/4/0 indicates two active routes, four received routes, and no damped routes. 	
BGP Neighbors		
Peer	Address of the BGP neighbor.	
AS	AS number of the peer.	
Type	Type of peer: Internal or External .	
State	<p>Current state of the BGP session:</p> <ul style="list-style-type: none"> ■ Active—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message. ■ Connect—BGP is waiting for the TCP connection to become complete. ■ Established—The BGP session has been established, and the peers are exchanging BGP update messages. ■ Idle—This is the first stage of a connection. BGP is waiting for a Start event. ■ OpenConfirm—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message. ■ OpenSent—BGP has sent an open message and is waiting to receive an open message from the peer. 	<p>Generally, the most common states are Active, which indicates a problem establishing the BGP connection, and Established, 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.</p>
Export	Names of any export policies configured on the peer.	
Import	Names of any import policies configured on the peer.	
Number of flaps	Number of times the BGP sessions has changed state from Down to Up .	A high number of flaps might indicate a problem with the interface on which the session is established.

Monitoring DLSw Routing Information

This feature is not currently supported.

Monitoring Class-of-Service Performance

The J-Web 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 following CLI command:

```
show class-of-service
```

This section contains the following topics:

- Monitoring CoS Interfaces on page 208
- Monitoring CoS Classifiers on page 209
- Monitoring CoS Value Aliases on page 210
- Monitoring CoS RED Drop Profiles on page 210
- Monitoring CoS Forwarding Classes on page 211
- Monitoring CoS Rewrite Rules on page 212
- Monitoring CoS Scheduler Maps on page 213

Monitoring CoS Interfaces

To display details about the physical and logical interfaces and the CoS components assigned to them, select **Monitor > Class of Service > Interfaces** in the J-Web interface, or enter the following CLI command:

```
show class-of-service interface interface
```

Table 154 on page 208 summarizes key output fields for CoS interfaces.

Table 154: 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.	

Table 154: Summary of Key CoS Interfaces Output Fields (*continued*)

Field	Values	Additional Information
Logical Interface	Name of a logical interface on the physical interface, to which CoS components are assigned.	
Object	Category of an object—for example, classifier, scheduler-map, or rewrite.	
Name	Name that you have given to an object—for example, ba-classifier .	
Type	Type of an object—for example, dscp , or exp for a classifier.	
Index	Index of this interface or the internal index of a specific object.	

Monitoring CoS Classifiers

To display the mapping of incoming CoS value to forwarding class and loss priority, for each classifier, select **Monitor > Class of Service > Classifiers** in the J-Web interface, or enter the following CLI command:

```
show class-of-service classifier
```

Table 155 on page 209 summarizes key output fields for CoS classifiers.

Table 155: Summary of Key CoS Classifier Output Fields

Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).
CoS Value Type	The classifiers are displayed by type: <ul style="list-style-type: none"> ■ dscp—All classifiers of the DSCP type. ■ dscp ipv6—All classifiers of the DSCP IPv6 type. ■ exp—All classifiers of the MPLS EXP type. ■ ieee-802.1—All classifiers of the IEEE 802.1 type. ■ inet-precedence—All classifiers of the IP precedence type. 	
Index	Internal index of the classifier.	
Incoming CoS Value	CoS value of the incoming packets, in bits. These values are used for classification.	

Table 155: Summary of Key CoS Classifier Output Fields (*continued*)

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

To display information about the CoS value aliases that the system is currently using to represent DSCP, DSCP IPv6, MPLS EXP, and IPv4 precedence bits, select **Monitor > Class of Service > CoS Value Aliases** in the J-Web interface, or enter the following CLI command:

```
show class-of-service code-point-aliases
```

Table 156 on page 210 summarizes key output fields for CoS value aliases.

Table 156: 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"> ■ dscp—Examines Layer 3 packet headers for IP packet classification. ■ dscp ipv6—Examines Layer 3 packet headers for IPv6 packet classification. ■ exp—Examines Layer 2 packet headers for MPLS packet classification. ■ ieee-802.1—Examines Layer 2 packet header for packet classification. ■ inet-precedence—Examines Layer 3 packet headers for IP packet classification. 	To display aliases and bit patterns, click the plus sign (+).
CoS Value Alias	Name given to a set of bits—for example, af11 is a name for 001010 bits.	
Bit Pattern	Set of bits associated with an alias.	

Monitoring CoS RED Drop Profiles

To display data point information for each CoS random early detection (RED) drop profile currently on a system, select **Monitor > Class of Service > RED Drop Profiles** in the J-Web interface, or enter the following CLI command:

show class-of-service drop-profile

Table 157 on page 211 summarizes key output fields for CoS RED drop profiles.

Table 157: Summary of Key CoS RED Drop Profile Output Fields

Field	Values	Additional Information
RED Drop Profile Name	Name of the RED drop profile. A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and one for drop probability, that determine the relationship between a buffer's fullness and the likelihood it will drop packets.	To display profile values, click the plus sign (+).
Graph RED Profile	Link to a graph of a RED curve that the system uses to determine the drop probability based on queue buffer fullness.	The x axis represents the queue buffer fill level, and the y axis represents the drop probability.
Type	Type of a specific drop profile: <ul style="list-style-type: none"> ■ interpolated—The two coordinates (x and y) of the graph are interpolated to produce a smooth profile. ■ segmented—The two coordinates (x and y) of the graph are represented by line fragments to produce a segmented profile. For information about types of drop profiles, see the <i>JUNOS Class of Service Configuration Guide</i> .	
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

To view the current assignment of CoS forwarding classes to queue numbers on the system, select **Monitor > Class of Service > Forwarding Classes** in the J-Web interface, or enter the following CLI command:

show class-of-service forwarding-class

Table 158 on page 212 summarizes key output fields for CoS forwarding classes.

Table 158: Summary of Key CoS Forwarding Class Output Fields

Field	Values	Additional Information
Forwarding Class	<p>Names of forwarding classes assigned to queue numbers. By default, the following forwarding classes are assigned to queues 0 through 3:</p> <ul style="list-style-type: none"> ■ best-effort—Provides no special CoS handling of packets. Loss priority is typically not carried in a CoS value, and RED drop profiles are more aggressive. ■ expedited-forwarding—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. ■ assured-forwarding—Provides high assurance for packets within specified service profile. Excess packets are dropped. ■ network-control—Packets can be delayed but not dropped. 	
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

To display information about CoS value rewrite rules, which are based on the forwarding class and loss priority, select **Monitor > Class of Service > Rewrite Rules** in the J-Web interface, or enter the following CLI command:

```
show class-of-service rewrite-rules
```

Table 159 on page 212 summarizes key output fields for CoS rewrite rules.

Table 159: Summary of Key CoS Rewrite Rules Output Fields

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	
CoS Value Type	<p>Rewrite rule type:</p> <ul style="list-style-type: none"> ■ dscp—For IPv4 DiffServ traffic. ■ dscp-ipv6—For IPv6 DiffServ traffic. ■ exp—For MPLS traffic. ■ ieee-802.1—For Layer 2 traffic. ■ inet-precedence—For IPv4 traffic. 	To display forwarding classes, loss priorities, and rewritten CoS values, click the plus sign (+).
Index	Internal index for this particular rewrite rule.	

Table 159: 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

To display assignments of CoS forwarding classes to schedulers, select **Monitor > Class of Service > Scheduler Maps** in the J-Web interface, or enter the following CLI command:

```
show class-of-service scheduler-map
```

Table 160 on page 213 summarizes key output fields for CoS scheduler maps.

Table 160: 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"> ■ A percentage—The scheduler receives the specified percentage of the total interface bandwidth. ■ remainder—The scheduler receives the remaining bandwidth of the interface after allocation to other schedulers. 	
Rate Limit	Rate limiting configuration of the queue: <ul style="list-style-type: none"> ■ none—No rate limiting. ■ exact—The queue transmits at only the configured rate. 	

Table 160: 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"> ■ A percentage—The buffer is a percentage of the total buffer allocation. ■ remainder—The buffer is sized according to what remains after other scheduler buffer allocations. 	
Priority	Scheduling priority of a queue: <ul style="list-style-type: none"> ■ high—Packets in this queue are transmitted first. ■ low—Packets in this queue are transmitted last. ■ medium-high—Packets in this queue are transmitted after high-priority packets. ■ medium-low—Packets in this queue are transmitted before low-priority packets. 	
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"> ■ low—Packet has a low loss priority. ■ high—Packet has a high loss priority. ■ medium-low—Packet has a medium-low loss priority. ■ medium-high—Packet has a medium-high loss priority. 	
Protocol	Transport protocol corresponding to a drop profile.	
Drop Profile Name	Name of the drop profile.	

Monitoring MPLS Traffic Engineering Information

The J-Web interface provides information about MPLS label-switched paths (LSPs) and virtual private networks (VPNs).

This section contains the following topics:

- Monitoring MPLS Interfaces on page 215
- Monitoring MPLS LSP Information on page 215
- Monitoring MPLS LSP Statistics on page 216

- Monitoring RSVP Session Information on page 217
- Monitoring MPLS RSVP Interfaces Information on page 218

Monitoring MPLS Interfaces

To view the interfaces on which MPLS is configured, including operational state and any administrative groups applied to an interface, select **Monitor > MPLS > Interfaces**, or enter the following CLI command:

```
show mpls interface
```

Table 161 on page 215 summarizes key output fields in the MPLS interface information display.

Table 161: 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: Up or Dn (down).	
Administrative groups	Administratively assigned colors of the MPLS link configured on the interface.	

Monitoring MPLS LSP Information

To view all label-switched paths (LSPs) configured on the services router, including all inbound (ingress), outbound (egress), and transit LSP information, select **Monitor > MPLS > LSP Information**, or enter the following CLI command:

```
show mpls lsp
```

Table 162 on page 215 summarizes key output fields in the MPLS LSP information display.

Table 162: 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.

Table 162: Summary of Key MPLS LSP Information Output Fields (*continued*)

Field	Values	Additional Information
To	Destination (outbound device) of the session.	
From	Source (inbound device) of the session.	
State	State of the path. It can be Up , Down , or AdminDn .	AdminDn 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 (inet.0). For transit and outbound RSVP sessions, the routing table is the primary MPLS table (mpls.0).
Active Path	Name of the active path: Primary or Secondary .	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 FF (fixed filter), SE (shared explicit), or WF (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— ingress (inbound), egress (outbound), or transit .	

Monitoring MPLS LSP Statistics

To display statistics for LSP sessions currently active on the device, including the total number of packets and bytes forwarded through an LSP, select **Monitor > MPLS > LSP Statistics**, or enter the following CLI command:

```
show mpls lsp statistics
```



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 163 on page 217 summarizes key output fields in the MPLS LSP statistics display.

Table 163: 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: Up, Down, or AdminDn.	AdminDn 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—ingress (inbound), egress (outbound), or transit.	

Monitoring RSVP Session Information

To view information about RSVP-signaled LSP sessions currently active on the device, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name, select **Monitor > MPLS > RSVP Sessions**, or enter the following CLI command:

```
show rsvp session
```

Table 164 on page 217 summarizes key output fields in the RSVP session information display.

Table 164: 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.

Table 164: Summary of Key RSVP Session Information Output Fields (*continued*)

Field	Values	Additional 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: Up , Down , or AdminDn .	AdminDn 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 (inet.0). For transit and outbound RSVP sessions, the routing table is the primary MPLS table (mpls.0).
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 FF (fixed filter), SE (shared explicit), or WF (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— ingress (inbound), egress (outbound), or transit .	

Monitoring MPLS RSVP Interfaces Information

To 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, select **Monitor > MPLS > RSVP Interfaces**, or enter the following CLI command:

```
show rsvp interface
```

Table 165 on page 218 summarizes key output fields in the RSVP interfaces information display.

Table 165: Summary of Key RSVP Interfaces Information Output Fields

Field	Values	Additional Information
RSVP Interface	Number of interfaces on which RSVP is active. Each interface has one line of output.	

Table 165: Summary of Key RSVP Interfaces Information Output Fields *(continued)*

Field	Values	Additional Information
Interface	Name of the interface.	
State	State of the interface: <ul style="list-style-type: none"> ■ Disabled—No traffic engineering information is displayed. ■ Down—The interface is not operational. ■ Enabled—Displays traffic engineering information. ■ Up—The interface is operational. 	
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 (static bandwidth X subscription factor).	
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).	

Monitoring PPPoE

The PPPoE monitoring information is displayed in multiple parts. To display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the device, and the PPPoE version configured on the device, select **Monitor > PPoE** in the J-Web interface.

To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

Alternatively, enter the following CLI commands:

- show pppoe interfaces
- show pppoe statistics
- show pppoe version

Table 166 on page 220 summarizes key output fields in PPPoE displays.

You can also view status information about the PPPoE interface by entering the **show interfaces pp0** command in the CLI editor. For more information about key output fields, see “Monitoring Interfaces” on page 149.

Table 166: Summary of Key PPPoE Output Fields

Field	Values	Additional Information
PPPoE Interfaces		
Interface	Name of the PPPoE interface. (See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i> .)	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.	
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, ge-0/0/0.1 .	
PPPoE Statistics		

Table 166: Summary of Key PPPoE Output Fields *(continued)*

Field	Values	Additional Information
Active PPPoE Sessions	Total number of active PPPoE sessions.	
Packet Type	<p>Packets sent and received during the PPPoE session, categorized by packet type and packet error:</p> <ul style="list-style-type: none"> ■ PADI—PPPoE Active Discovery Initiation packets. ■ PADO—PPPoE Active Discovery Offer packets. ■ PADR—PPPoE Active Discovery Request packets. ■ PADS—PPPoE Active Discovery Session-Confirmation packets. ■ PADT—PPPoE Active Discovery Terminate packets. ■ Service Name Error—Packets for which the Service-Name request could not be honored. ■ AC System Error—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. ■ Generic Error—Packets that indicate an unrecoverable error occurred. ■ Malformed Packet—Malformed or short packets that caused the packet handler to disregard the frame as unreadable. ■ Unknown Packet—Unrecognized packets. 	
Sent	Number of the specific type of packet sent from the PPPoE client.	
Received	Number of the specific type of packet received by the PPPoE client.	
Timeout	<p>Information about the timeouts that occurred during the PPPoE session.</p> <ul style="list-style-type: none"> ■ PADI—Number of timeouts that occurred for the PADI packet. ■ PADO—Number of timeouts that occurred for the PADO packet. (This value is always 0 and is not supported.) ■ PADR—Number of timeouts that occurred for the PADR packet. 	
Sent	Number of the timeouts that occurred for PADI, PADO, and PADR packets.	
PPPoE Version		

Table 166: Summary of Key PPPoE Output Fields (*continued*)

Field	Values	Additional Information
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.	

Monitoring PPP

PPP monitoring information includes 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 interface does not include pages for displaying PPP monitoring information.

To display PPP monitoring information, enter the following CLI commands:

- `show ppp address-pool pool-name`
- `show ppp interface interface-name`

- show ppp statistics
- show ppp summary

For information about these CLI commands, see the *JUNOS Interfaces Command Reference*.

Monitoring the WAN Acceleration Interface

To view status information and traffic statistics for the WAN acceleration interface, select **Monitor > WAN Acceleration** in the J-Web interface, or select **Monitor > Interfaces** and select the interface name (`wx-slot/0/0`). Alternatively, enter the following CLI command:

```
show interfaces wx-slot/0/0 detail
```

For a description of the interface properties and statistics, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Monitoring Services

Monitoring DHCP

This section contains the following topics:

- Monitoring DHCP Service Statistics on page 223
- Monitoring DHCP Client Bindings on page 224
- Monitoring DHCP Conflicts on page 225
- Monitoring DHCP Clients on page 225
- Monitoring DHCP Relay Statistics on page 226

Monitoring DHCP Service Statistics

A J Series or SRX Series device can operate as a Dynamic Host Configuration Protocol (DHCP) server. To view information about global scope and DHCP service statistics, select **Monitor > Services > DHCP > Statistics** in the J-Web interface, or enter the following CLI commands:

- show system services dhcp global
- show system services dhcp statistics

Table 167 on page 223 summarizes the key output fields in the DHCP service statistics displays.

Table 167: Summary of Key Global Scope and DHCP Service Statistics Output Fields

Field	Values	Additional Information
Global Information Summary		

Table 167: Summary of Key Global Scope and DHCP Service Statistics Output Fields *(continued)*

Field	Values	Additional Information
BOOTP Lease Length	Length of the BOOTP lease.	
DHCP Options		
Server Identifier	IP address of the name server.	
Name Server	IP address of the name server.	
Router	IP address of the name router.	
Domain Name	Name of the domain.	
DHCP Lease Time		
Default Lease Time	Lease time assigned to clients that do not request a specific lease time.	
Minimum Lease Time	Minimum time a client can retain an IP address lease on the server.	
Maximum Lease Time	Maximum time a client can retain an IP address lease on the server.	
Total Dropped packets	Total number of packets dropped and the number of packets dropped due to a particular condition.	
Messages Received	Number of BOOTREQUEST, DHCPDECLINE, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.	
Messages Sent	Number of BOOTREPLY, DHCPOFFER, DHCPACK, and DHCPNAK messages sent from the DHCP server to DHCP clients.	

Monitoring DHCP Client Bindings

To view information about DHCP client bindings, select **Monitor > Services > DHCP > Binding** in the J-Web interface, or enter the following CLI command:

```
■ show system services dhcp binding
```

Table 168 on page 225 summarizes the key output fields in the DHCP client binding displays.

Table 168: 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 never for leases that do not expire.	

Monitoring DHCP Conflicts

To view information about DHCP address conflicts, select **Monitor > Services > DHCP > Conflicts** in the J-Web interface, or enter the following CLI command:

- `show system services dhcp conflict`

Table 169 on page 225 summarizes the key output fields in the DHCP conflict displays.

Table 169: Summary of Key DHCP Conflict Statistics Output Fields

Field	Values	Additional Information
Detection Time	Date and time the client detected the conflict.	
Detection Method	How the conflict was detected.	Only client-detected conflicts are displayed.
IP Address	IP address where the conflict occurred.	The address in the conflicts list remains excluded until you use the <code>clear system services dhcp</code> command to manually clear the list.

Monitoring DHCP Clients

To view information about DHCP clients, select **Monitor > Services > DHCP > Client** in the J-Web interface, or enter the following CLI command:

- `show system services dhcp client`

Table 170 on page 226 summarizes the key output fields in the DHCP client displays.

Table 170: Summary of Key DHCP Client Output Fields

Field	Values	Additional Information
Interface	Name of the logical interface.	
Obtained at	Date and time the lease was obtained.	
Hardware Address	MAC address of the interface.	
Status	State of the client binding.	
Address obtained	IP address obtained from the DHCP server.	
Update Server	Displayed if the propagation of TCP/IP settings are enabled on the specified interface (if it is acting as a DHCP client) to the DHCP server configured on the device.	
Lease obtained at	Date and time the lease was obtained.	
Lease Expires at	Date and time the lease expires.	

Monitoring DHCP Relay Statistics

To view information about DHCP relay statistics, select **Monitor > Services > DHCP > Relay Statistics** in the J-Web interface or enter the following CLI command:

```
show system services dhcp relay-statistics
```

Table 171 on page 226 summarizes the key output fields in the DHCP relay statistics displays.

Table 171: Summary of Key DHCP Relay Statistics Output Fields

Field	Values	Additional Information
Received Packets	Total DHCP packets received.	
Forwarded Packets	Total DHCP packets forwarded.	

Table 171: Summary of Key DHCP Relay Statistics Output Fields *(continued)*

Field	Values	Additional Information
Dropped packets	Total DHCP packets dropped for the following reasons: <ul style="list-style-type: none">■ Missing interface in the relay database■ Missing matching routing instance■ Error during packet read■ Error during packet send■ Invalid server address■ Missing valid local address■ Missing route to the server or client	

Chapter 14

Monitoring Events and Managing System Log Files

JUNOS Software 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. The View Events page on the J-Web interface enables you to filter and view system log messages.

For more information about system log messages, see the *JUNOS System Log Messages Reference*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics:

- System Log Message Terms on page 229
- System Log Messages Overview on page 231
- Before You Begin on page 233
- Configuring System Log Messages with a Configuration Editor on page 234
- Monitoring System Log Messages with the J-Web Event Viewer on page 236

System Log Message Terms

Before configuring and monitoring system log messages, become familiar with the terms defined in Table 172 on page 229.

Table 172: System Log Message Terms

Term	Definition
event	Condition that occurs on a device at a particular time. An event can include routine, failure, error, emergency or critical conditions.
event ID	System log message code that uniquely identifies a system log message. The code begins with a prefix indicating the software process or library that generates the event.
facility	Group of messages that either are generated by the same software process (such as accounting statistics) or concern a similar condition or activity (such as authentication attempts). For a list of system logging facilities, see Table 173 on page 232.

Table 172: System Log Message Terms (*continued*)

Term	Definition
priority	Combination of the facility and severity level of a system log message. By default, priority information is not included in system log messages, but you can configure JUNOS Software to include it. For more information, see the <i>JUNOS System Log Messages Reference</i> . See also <i>facility</i> ; <i>severity level</i> .
process	<p>Software program, also known as a daemon, that controls device functionality. The following are the primary JUNOS Software processes:</p> <ul style="list-style-type: none"> ■ Routing protocol process (rpd)—Defines how routing protocols such as RIP, OSPF, and BGP operate on the device. It starts the configured routing protocols, handles all routing messages, maintains routing tables and implements the routing policy. ■ Interface process (also called device control process) (dcd)—Allows you to configure and control the physical and logical interfaces present in a device. It also enables JUNOS Software to track the status and condition of the device's interfaces. ■ Chassis process (chassisd)—Controls the physical properties of a device chassis, including conditions that trigger alarms. ■ SNMP—Simple Network Management Protocol, which helps administrators monitor the state of a device. ■ Management process (mgd)—Controls processes that start and monitor all the other software processes. The management process starts the command-line interface (CLI), which is the primary tool used to control and monitor JUNOS Software. It also starts all the software processes and the CLI when the device starts up. If a software process terminates, the management process attempts to restart it. ■ Forwarding process (flowd)—Forwards packets through the device. The flow-based forwarding process applies filters and policers associated with the ingress interface to packets entering the device. It establishes the state of the packet's session and manages the packet as it transits the security flow and its applicable features. It applies output filtering and traffic shaping to the flow before transmitting the packet out the egress interface. ■ Network security process (nsd)—Interprets, executes, and manages the configuration of extended interface attributes, policies, zones, address books, firewall screens, Network Address Translation (NAT), and other network security treatments. ■ Internet Key Exchange process (iked)—Implements tunnel management for IPSec VPNs, provides authentication of endpoint entities, and generates keys for packet authentication and encryption. ■ Firewall authentication process (fwauthd)—Implements and manages user authentication configuration, and authenticates users who access the firewall. ■ Dynamic Host Configuration Protocol process (dhcpcd)—Implements the DHCP client, allowing the device to obtain IP addresses from the network DHCP server, set other configuration parameters, manage TCP/IP settings propagation, and display client-related information. <p>For more information about processes, see the <i>JUNOS Software Installation and Upgrade Guide</i>.</p>
process ID	Identifier uniquely identifying a process. The process ID is displayed in a system log message along with the name of the process that generates the event.
severity level	Measure of how seriously a triggering event affects device functions. For a list of severity levels that you can specify, see Table 174 on page 232.

System Log Messages Overview

JUNOS Software generates system log messages (also called *syslog messages*) to record events that occur on the device, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as device power-off due to excessive temperature

The JUNOS system logging utility is similar to the UNIX `syslogd` utility. Each system log message identifies the software process that generated the message and briefly describes the operation or error that occurred.

Reboot requests are recorded to the system log files, which you can view with the `show log` command. Also, you can view the names of any processes running on your system with the `show system processes` command.

System Log Message Destinations

You can send system logging information to one or more destinations. The destinations can be one or more files, one or more remote hosts, the terminals of one or more users if they are logged in, and the system console.

- To direct messages to a named file in a local file system, see “Sending System Log Messages to a File” on page 234.
- To direct messages to the terminal session of one or more specific users (or all users) when they are logged into the device, see “Sending System Log Messages to a User Terminal” on page 235.
- To send a security log stream to a remote server, see “Sending System Log Messages to a Remote Server” on page 235
- To direct messages to the device console, see the *JUNOS System Log Messages Reference*.
- To direct messages to a remote machine that is running the UNIX `syslogd` utility, see the *JUNOS System Log Messages Reference*.

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 (see “Sending System Log Messages to a Remote Server” on page 235). 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.

System Log Facilities and Severity Levels

When specifying the destination for system log messages, you can specify the class (facility) of messages to log and the minimum severity level (level) of the message for each location.

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.

Table 173 on page 232 lists the system logging facilities, and Table 174 on page 232 lists the system logging severity levels. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Table 173: System Logging Facilities

Facility	Description
any	Any facility
authorization	Any authorization attempt
change-log	Any change to the configuration
cron	Cron scheduling process
daemon	Various system processes
interactive-commands	Commands executed in the CLI
kernel	Messages generated by the JUNOS kernel
user	Messages from random user processes

Table 174: System Logging Severity Levels

Severity Level (from Highest to Lowest Severity)	Description
emergency	System panic or other conditions that cause the routing platform to stop functioning.
alert	Conditions that must be corrected immediately, such as a corrupted system database.
critical	Critical conditions, such as hard drive errors.
error	Standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
warning	Conditions that warrant monitoring.

Table 174: System Logging Severity Levels (*continued*)

Severity Level (from Highest to Lowest Severity)	Description
notice	Conditions that are not error conditions but are of interest or might warrant special handling.
info	Informational messages. This is the default.
debug	Software debugging messages.

Control and Data Plane Logs

JUNOS Software 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 policies and/or by generating system log messages. 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. How the system handles data plane events depends on the device:
 - For J Series devices, 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 SRX Series devices, the system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. If an event requires processing, the system sends the event to the **eventd** process on the Routing Engine.

To view data plane logs, use the **log** statement at the **[security]** hierarchy level.

Before You Begin

Before you begin configuring and monitoring system log messages, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See the *JUNOS Software Interfaces and Routing Configuration Guide*.

Configuring System Log Messages with a Configuration Editor

This section contains the following topics:

- Sending System Log Messages to a File on page 234
- Sending System Log Messages to a User Terminal on page 235
- Sending System Log Messages to a Remote Server on page 235
- Archiving System Logs on page 236
- Disabling System Logs on page 236

Sending System Log Messages to a File

You can direct system log messages to a file on the CompactFlash card. The default directory for log files is `/var/log`. To specify a different directory on the CompactFlash card, include the complete pathname. For the list of logging facilities and severity levels, see Table 173 on page 232 and Table 174 on page 232.

For information about archiving log files, see “Archiving System Logs” on page 236.

The procedure provided in this section sends all security-related information to the sample file named `security`.

To send messages to a file:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 175 on page 234.
3. If you are finished configuring the network, commit the configuration.

Table 175: Sending System Log Messages to a File

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Syslog level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Syslog, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p><code>edit system syslog</code></p>
Create a file named <code>security</code> , and send log messages of the <code>authorization</code> class at the severity level <code>info</code> to the file.	<ol style="list-style-type: none"> 1. Next to File, click Add new entry. 2. In the File name box, type <code>security</code>. 3. Next to Contents, click Add new entry. 4. In the Facility list, select authorization. 5. In the Level list, select info. 	<p>Set the filename and the facility and severity level:</p> <p><code>set file security authorization info</code></p>

Sending 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 into the local Routing Engine, specify one or more JUNOS usernames. Separate multiple values with spaces, or use the asterisk (*) to indicate all users who are logged into the local Routing Engine. For the list of logging facilities and severity levels, see Table 173 on page 232 and Table 174 on page 232.

The procedure provided in this section sends any critical messages to the terminal of the sample user **frank**, if he is logged in.

To send messages to a user terminal:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 176 on page 235.
3. If you are finished configuring the network, commit the configuration.

Table 176: Sending Messages to a User Terminal

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Syslog level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to System, click Configure or Edit. 3. Next to Syslog, click Configure or Edit. 	<p>From the [edit] hierarchy level, enter</p> <p>edit system syslog</p>
Send all critical messages to the user frank .	<ol style="list-style-type: none"> 1. Next to User, click Add new entry. 2. In the User name box, type frank. 3. Next to Contents, click Add new entry. 4. In the Facility list, select any. 5. In the Level list, select critical. 	<p>Set the filename and the facility and severity level:</p> <p>set user frank any critical</p>

Sending System Log Messages to a Remote Server

To enable a device to send system logs to a remote server, enter the following command:

```
{primary:node0}
user@host> set security log stream name host URL / IP address
```

To allow a duplicate log to be sent to a second remote server, repeat the command with a new stream name and the URL or IP address of the second server. Note that attempting to run the command a third time will return an error.



NOTE: If your deployment is an active/active chassis cluster, you can also configure one security log stream on each active node to separate remote servers and likewise achieve logging redundancy.

If you need to rename or redirect one of the streams, you will need to delete and re-create it. To delete a security log stream, enter the following command:

```
{primary:node0}
user@host> delete security log stream name
```

Archiving System Logs

By default, the JUNOS logging utility stops writing messages to a log file when the file reaches 128 KB in size. It closes the file and adds a numerical suffix, then opens and directs messages to a new file with the original name. By default, the logging utility creates up to 10 files before it begins overwriting the contents of the oldest file. The logging utility by default also limits the users who can read log files to the root user and users who have the JUNOS maintenance permission.

To enable all users to read log files, include the **world-readable** statement at the **[edit system syslog archive]** hierarchy level. To restore the default permissions, include the **no-world-readable** statement. You can include the **archive** statement at the **[edit system syslog file filename]** hierarchy level to configure the number of files, file size, and permissions for the specified log file. For configuration details, see the information about archiving log files in the *JUNOS System Basics Configuration Guide*.

Disabling System Logs

To disable logging of the messages from a facility, use the **facility none** configuration statement. This statement is useful when, for example, you want to log messages of the same severity level from all but a few facilities. Instead of including a configuration statement for each facility you want to log, you can configure the **any level** statement and then a **facility none** statement for each facility you do not want to log. For configuration details, see the information about disabling logging in the *JUNOS System Basics Configuration Guide*.

Monitoring System Log Messages with the J-Web Event Viewer

To monitor errors and events that occur on the device, select **Monitor > Events and Alarms > View Events** in the J-Web user interface.

The J-Web View Events page displays the following information about each event:

- **Process**—System process that generated the error or event.
- **Severity**— A severity level indicates how seriously the triggering event affects routing platform functions. Only messages from the facility that are rated at that level or higher are logged. Possible severities and their corresponding color code are:

- Debug/Info/Notice (Green)—Indicates conditions that are not errors but are of interest or might warrant special handling.
- Warning (Yellow)—Indicates conditions that warrant monitoring.
- Error (Blue)—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- Critical (Pink)—Indicates critical conditions, such as hard drive errors.
- Alert (Orange)—Indicates conditions that require immediate correction, such as a corrupted system database.
- Emergency (Red)—Indicates system panic or other conditions that cause the routing platform to stop functioning.
- Event ID—Unique ID of the error or event. The prefix on each code identifies the generating software process. The rest of the code indicates the specific event or error.
- Event Description—Displays a more detailed explanation of the message.
- Time—Time that the error or event occurred.

To control which errors and events are displayed in the list, use the following options:

- System Log File—Specify the name of the system log file that records the errors and events.
- Process—Specify the system processes that generate the events you want to display. For an overview of some of the primary system processes, see Table 172 on page 229. 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. For a complete list of system error and event IDs, see the *JUNOS Software System Log Messages Reference*.
- 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.

Chapter 15

Configuring and Monitoring Alarms

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 interface or the CLI.

For more information about alarms, see the *JUNOS System Basics Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Alarm Terms on page 239
- Alarm Overview on page 240
- Before You Begin on page 245
- Configuring Alarms with a Configuration Editor on page 245
- Checking Active Alarms on page 247
- Verifying the Alarms Configuration on page 247

Alarm Terms

Before configuring and monitoring alarms, become familiar with the terms defined in Table 177 on page 239.

Table 177: Alarm Terms

Term	Definition
alarm	Signal alerting you to conditions that might prevent normal operation. The alarm signal is the yellow ALARM LED lit on the front of the chassis.
alarm condition	Failure event that triggers an alarm.
alarm severity	Seriousness of the alarm. The level of severity can be either major (red) or minor (yellow).

Table 177: Alarm Terms *(continued)*

Term	Definition
chassis alarm	Predefined alarm triggered by a physical condition on the device such as a power supply failure, excessive component temperature, or media failure.
interface alarm	<p>Alarm triggered by the state of a physical link on a fixed or installed Physical Interface Module (PIM), such as a link failure or a missing signal.</p> <p>Interface alarms are triggered by conditions on a T1 (DS1), Fast Ethernet, serial, or T3 (DS3) physical interface or by conditions on the sp-0/0/0 adaptive services interface for stateful firewall filter, Network Address Translation (NAT), Intrusion Detection and Prevention (IDP), or IP Security (IPsec) services.</p> <p>To enable an interface alarm, you must explicitly set an alarm condition.</p>
system alarm	Predefined alarm triggered by a missing rescue configuration or failure to install a license for a licensed software feature.

Alarm Overview

Alarms warn you about conditions that can prevent the device from operating normally.

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 240
- Alarm Severity on page 241
- Alarm Conditions on page 241

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 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 or CLI display.

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 241
- System Alarm Conditions and Corrective Actions on page 244

Interface Alarm Conditions

Table 178 on page 242 lists the interface conditions, sorted by interface type, that you can configure for an alarm. Each alarm condition can be configured 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 178: Interface Alarm Conditions

Interface	Alarm Condition	Description	Configuration Option
DS1 (T1)	Alarm indication signal (AIS)	The normal T1 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	ylw
Ethernet	Link is down	The physical link is unavailable.	link-down
Integrated services	Hardware or software failure	On the adaptive services module, either the hardware associated with the module or the software that drives the module has failed.	failure
Serial	Clear-to-send (CTS) signal absent	The remote endpoint of the serial link is not transmitting a CTS signal. The CTS signal must be present before data can be transmitted across a serial link.	cts-absent
	Data carrier detect (DCD) signal absent	The remote endpoint of the serial link is not transmitting a DCD signal. Because the DCD signal transmits the state of the device, no signal probably indicates that the remote endpoint of the serial link is unavailable.	dcd-absent
	Data set ready (DSR) signal absent	The remote endpoint of the serial link is not transmitting a DSR signal. The DSR signal indicates that the remote endpoint is ready to receive and transmit data across the serial link.	dsr-absent
	Loss of receive clock	The clock signal from the remote endpoint is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-rx-clock
	Loss of transmit clock	The local clock signal is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-tx-clock

Table 178: Interface Alarm Conditions *(continued)*

Interface	Alarm Condition	Description	Configuration Option
Services	Services module hardware down	A hardware problem has occurred on the device's services module. This error typically means that one or more of the CPUs on the module has failed.	hw-down
	Services link down	The link between the device and its services module is unavailable.	linkdown
	Services module held in reset	The device's services module is stuck in reset mode. If the services module fails to start up five or more times in a row, the services module is held in reset mode. Startup fails when the amount of time from CPU release to CPU halt is less than 300 seconds.	pic-hold-reset
	Services module reset	The device's services module is resetting. The module resets after it crashes or is reset from the CLI, or when it takes longer than 60 seconds to start up.	pic-reset
	Services module software down	A software problem has occurred on the device's services module.	sw-down
E3	Alarm indication signal (AIS)	The normal E3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Loss of signal (LOS)	No remote E3 signal is being received at the E3 interface.	los
	Out of frame (OOF)	An OOF condition has existed for 10 seconds. This alarm applies only to E3 interfaces configured in frame mode. The OOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds.	oof
	Remote defect indication	An AIS, LOS, or OOF condition exists. This alarm applies only to E3 interfaces configured in frame mode.	rdi

Table 178: Interface Alarm Conditions (*continued*)

Interface	Alarm Condition	Description	Configuration Option
T3 (DS3)	Alarm indication signal	The normal T3 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Excessive number of zeros	The bit stream received from the upstream host has more consecutive zeros than are allowed in a T3 frame.	exz
	Far-end receive failure (FERF)	The remote endpoint of the connection has failed. A FERF differs from a yellow alarm, because the failure can be any failure, not just an OOF or LOS failure.	ferf
	Idle alarm	The Idle signal is being received from the remote endpoint.	idle
	Line code violation	Either the line encoding along the T3 link is corrupted or a mismatch between the encoding at the local and remote endpoints of a T3 connection occurred.	lcv
	Loss of frame (LOF)	An OOF or loss-of-signal LOS condition has existed for 10 seconds. The LOF failure is cleared when no OOF or LOS defects have occurred for 20 seconds. A LOF failure is also called a red failure.	lof
	Loss of signal	No remote T3 signal is being received at the T3 interface.	los
	Phase-locked loop out of lock	The clocking signals for the local and remote endpoints no longer operate in lock-step.	pll
	Yellow alarm	The remote endpoint is in yellow alarm failure. This condition is also known as a far-end alarm failure.	ylw

System Alarm Conditions and Corrective Actions

Table 179 on page 244 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 179: System Alarm Conditions and Corrective Actions

Alarm Type	Alarm Condition	Corrective Action
Configuration	The rescue configuration is not set.	Set the rescue configuration. For instructions, see the <i>JUNOS CLI User Guide</i> .

Table 179: System Alarm Conditions and Corrective Actions (continued)

Alarm Type	Alarm Condition	Corrective Action
License	<p>You have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed.</p> <p>NOTE: This alarm indicates that you are in violation of the software license agreement. You must install a valid license key to be in compliance with all agreements.</p>	Install a valid license key. For instructions, see the <i>JUNOS Software Administration Guide</i> .

Before You Begin

Before you begin configuring and monitoring alarms, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See the *JUNOS Software Interfaces and Routing Configuration Guide*.

Configuring Alarms with a Configuration Editor

To configure interface alarms on a device, you must select the network interface on which to apply an alarm and the condition you want to trigger the alarm. For a list of conditions, see “Interface Alarm Conditions” on page 241.

To configure interface alarms:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 180 on page 245.
3. If you are finished configuring the network, commit the configuration.
4. To verify the alarms configuration, see “Displaying Alarm Configurations” on page 247.
5. To check the status of active alarms, see “Checking Active Alarms” on page 247.

Table 180: Configuring Interface Alarms

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Alarm level in the configuration hierarchy.	<ol style="list-style-type: none">1. In the J-Web interface, select CLI Tools > Point and Click CLI.2. Next to Chassis, click Configure or Edit.3. Next to Alarm, click Configure or Edit.	From the [edit] hierarchy level, enter edit chassis alarm

Table 180: Configuring Interface Alarms (*continued*)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the system to generate a red interface alarm when a yellow alarm is detected on a T1 (DS1) link.	<ol style="list-style-type: none"> 1. In the Ds1 field, click Configure. 2. From the Ylw list, select red. 3. Click OK. 	<p>Enter</p> <p>set ds1 ylw red</p>
Configure the system to generate a red interface alarm when a link down failure is detected on an Ethernet link.	<ol style="list-style-type: none"> 1. In the Ethernet field, click Configure. 2. From the Link down list, select red. 3. Click OK. 	<p>Enter</p> <p>set ethernet link-down red</p>
Configure the system to generate the following interface alarms on a serial link: <ul style="list-style-type: none"> ■ Yellow alarm when no CTS signal is detected ■ Yellow alarm when no DCD signal is detected ■ Red alarm when the receiver clock is not detected ■ Red alarm when the transmission clock is not detected 	<ol style="list-style-type: none"> 1. In the Serial field, click Configure. 2. From the Cts absent list, select yellow. 3. From the Dcd absent list, select yellow. 4. From the Loss of rx clock list, select red. 5. From the Loss of tx clock list, select red. 6. Click OK. 	<ol style="list-style-type: none"> 1. Enter set serial cts-absent yellow 2. Enter set serial dcd-absent yellow 3. Enter set serial loss-of-rx-clock red 4. Enter set serial loss-of-tx-clock red
Configure the system to generate the following interface alarms on a T3 link: <ul style="list-style-type: none"> ■ Red alarm when the remote endpoint is experiencing a Red failure ■ Yellow alarm when the upstream bit stream has more consecutive zeros than are permitted ■ Red alarm when there is a loss of signal on the interface 	<ol style="list-style-type: none"> 1. In the T3 field, click Configure. 2. From the Ylw list, select red. 3. From the Exz list, select yellow. 4. From the Los list, select red. 5. Click OK. 	<ol style="list-style-type: none"> 1. Enter set t3 ylw red 2. Enter set t3 exz yellow 3. Enter set t3 los red
Configure the system to display active system alarms whenever a user with the login class admin logs in to the device. To define login classes, see the <i>JUNOS System Basics Configuration Guide</i> .	<ol style="list-style-type: none"> 1. On the main Configuration page next to System, click Configure or Edit. 2. Next to Login, click Configure or Edit. 3. In the Class field, click Add new entry. 4. In the Class name field, type admin. 5. Select the Login alarms check box. 6. Click OK. 	<ol style="list-style-type: none"> 1. Enter edit system login 2. Enter set class admin login-alarms

Checking Active Alarms

To monitor alarms on the device, select **Monitor > Events and Alarms > View Alarms** in the J-Web user interface. The J-Web View Alarms page displays information about preset system and chassis alarms. (For information about interface alarms, see “Interface Alarm Conditions” on page 241.)

Alternatively, you can enter the following **show** commands in the CLI editor:

- **show chassis alarms**
- **show system alarms**

The J-Web View Alarms page displays the following information about each alarm:

- **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 are displayed, use the following options:

- **Alarm Type**—Specify 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. (For more information, see “Alarm Types” on page 240.)
- **Severity**—Specify 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. (For more information, see “Alarm Severity” on page 241.)
- **Description**—Enter a brief synopsis of the alarms you want to monitor.
- **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.
- **Go**—Executes the options that you specified.
- **Reset**—Clears the options that you specified.

Verifying the Alarms Configuration

To verify alarms configuration, perform the following task.

Displaying Alarm Configurations

Purpose Verify the configuration of the alarms.

Action From the J-Web interface, select **CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the `show chassis alarms` command.

```
[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;
}
```

Meaning The sample output in this section displays the following alarm settings (in order). Verify that the output shows the intended configuration of the alarms.

- T3 alarms
- DS1 alarms
- Ethernet alarms
- Serial alarms

Related Topics For more information about the format of a configuration file, see the *J-Web Interface User Guide* or the *JUNOS CLI User Guide*.

Part 4

Managing Device Software

- Performing Software Upgrades and Reboots on page 251
- Understanding and Changing Secure and Router Contexts on page 275
- Configuring Selective Stateless Packet-Based Services on page 289
- Installing and Managing Licenses on page 313
- Managing Files on page 323

Chapter 16

Performing Software Upgrades and Reboots

J Series Services Routers and SRX Series Services Gateways are delivered with JUNOS Software 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 your software to use them. Before an upgrade, we recommend that you back up your primary boot device.

On a services router, 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 or SRX Series device does not have a secondary boot device configured and the primary boot device becomes corrupted, you can reload the JUNOS recovery software package onto the corrupted CompactFlash card with either a UNIX or Microsoft Windows computer.



NOTE: The terms *JUNOS Software (legacy services)* and *JUNOS Software* are used frequently in this chapter. JUNOS Software (legacy services) denotes the packet-based software for the J Series Services Router, whereas JUNOS Software denotes the flow-based software for the J Series Services Router.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Upgrade and Downgrade Overview on page 252
- Before You Begin on page 253
- Downloading Software Upgrades from Juniper Networks on page 254
- Installing Software Upgrades on page 254
- Installing Software Upgrades Using the CLI on page 257

- Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway on page 259
- Downgrading the Software on page 262
- Configuring Boot Devices on page 263
- Rebooting or Halting the Device on page 269
- Bringing Chassis Components Online and Offline on page 272
- Chassis Control Restart Options on page 273

Upgrade and Downgrade Overview

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 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 Software is delivered in signed packages that contain digital signatures to ensure official Juniper Networks software. For more information about signed software packages, see the *JUNOS Software Installation and Upgrade Guide*.

Upgrade Software Packages

An upgrade software package name is in the following format:
package-name-m.nZx-distribution.tgz.

- *package-name* is the name of the package—for example, *junos-jsr*.
- *m.n* is the software release, with *m* representing the major release number and *n* representing the minor release number—for example, *8.5*.
- *Z* indicates the type of software release. For example, *R* indicates released software, and *B* indicates beta-level software.
- *x.y* represents the software build number and spin number—for example, *1.1*.
- *distribution* indicates the area for which the software package is provided—*domestic* for the United States and Canada and *export* for worldwide distribution.

A sample J Series upgrade software package name is *junos-jsr-8.5R1.1-domestic.tgz*.

Recovery Software Packages

Download a recovery software package, also known as an install media package, to recover a primary CompactFlash card.

A recovery software package name is in the following format:
package-name-m.nZx-export-cfnnn.gz.

- *package-name* is the name of the package—for example, *junos-jsr*.
- *m.n* is the software release, with *m* representing the major release number—for example, 8.5.
- *Z* indicates the type of software release. For example, *R* indicates released software, and *B* indicates beta-level software.
- *x.y* represents the software build number and spin number—for example, 1.1.
- *export* indicates that the recovery software package is the exported worldwide software package version.
- *cfnnn* indicates the size of the target CompactFlash card in megabytes—for example, *cf256*.

The following CompactFlash card sizes are supported:

- 256 MB
- 512 MB
- 1024 MB

CompactFlash cards with 128 MB of storage capacity are not supported.

A sample J Series recovery software package name is *junos-jsr-8.5R1.1-export-cf256.gz*.

Before You Begin

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

Before an upgrade, back up your primary boot device onto a secondary storage device. If you have a power failure during an upgrade, the primary boot device can fail or become corrupted. In either case, if a backup device is not available, the device might be unable to boot and come back online. 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.

During a successful upgrade, the upgrade package completely reinstalls the existing software. It retains configuration files, log files, and similar information from the previous version.

Use either the J-Web interface or the CLI to back up the primary boot device on the secondary storage device listed in Table 181 on page 254.

Table 181: Secondary Storage Devices for Backup

Storage Device	Available on Routers	Minimum Storage Required
External CompactFlash card	J2320 and J2350	256 MB
USB storage device	All services routers	256 MB

After a successful upgrade, remember to back up the new current configuration to the secondary device.

For instructions about how to backup your system using the J-Web Interface, see “Configuring a Boot Device for Backup with the J-Web Interface” on page 264. For instructions about how to backup your system using the CLI, see “Configuring a Boot Device for Backup with the CLI” on page 266.

Downloading Software Upgrades from Juniper Networks

Follow these steps 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. For information about JUNOS Software packages, see “Upgrade and Downgrade Overview” on page 252.
4. Download the software to a local host or to an internal software distribution site.

Installing Software Upgrades

Use either the J-Web interface or the CLI to upgrade from one software release to another.



NOTE: For more information on migrating a J Series Services Router to a later version of JUNOS Software, see the *JUNOS Software Migration Guide*.



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

This section contains the following topics:

- Installing Software Upgrades with the J-Web Interface on page 255

Installing Software Upgrades with the J-Web Interface

You can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or, if necessary, by uploading the software image to the device. This section contains the following topics:

- Installing Software Upgrades from a Remote Server on page 255
- Installing Software Upgrades by Uploading Files on page 256

Installing Software Upgrades from a Remote Server

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



NOTE: This procedure applies only to upgrading one JUNOS Software release to another or one JUNOS Software services release to another. To upgrade from the JUNOS Software to JUNOS Software services, see the *JUNOS Software Migration Guide*.

Figure 8 on page 255 shows the Install Remote page for the device.

Figure 8: Install Remote Page

[Manage](#) > [Software](#) > [Install Package](#)

Software

Install Package

You can instruct the router to retrieve a software package from a remote server by specifying the location below.

• **Package Location** ?

User ?

Password ?

Reboot If Required ☐ ?

To install software upgrades from a remote server:

1. Before installing the software upgrade, verify the available space on the CompactFlash card. For information about verifying available CompactFlash card space, see the *JUNOS Software Release Notes*.
2. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 254.
3. In the J-Web interface, select **Maintain > Software > Install Package**.
4. On the Install Remote page, enter the required information into the fields described in Table 182 on page 256.
5. Click **Fetch and Install Package**. The software is activated after the device reboots.

Table 182: 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: <code>ftp://hostname/pathname/package-name</code> <code>http://hostname/pathname/package-name</code>
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	If this box is checked, 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.

Installing Software Upgrades by Uploading Files

You can use the J-Web interface to install software packages uploaded from your computer. Before installing the software upgrade, you need to verify that there is enough available space on the CompactFlash card.



NOTE: This procedure applies only to upgrading one JUNOS Software release to another or one JUNOS Software services release to another. To upgrade from JUNOS Software to JUNOS Software services, see the *JUNOS Software Migration Guide*.

Figure 9 on page 257 shows the Upload Package page for the device.

Figure 9: Upload Package Page

[Manage](#) > [Software](#) > [Upload Package](#)

Software

Upload Package

The software package file specified below will be uploaded to the router for installation.

* File to Upload ?

Reboot If Required ☐ ?

To install software upgrades by uploading files:

1. Before installing the software upgrade, verify the available space on the CompactFlash card. For information about verifying available CompactFlash card space, see the *JUNOS Software Release Notes*.
2. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 254.
3. In the J-Web interface, select **Maintain > Software > Upload Package**.
4. On the Upload Package page, enter information into the fields described in Table 183 on page 257.
5. Click **Upload Package**. The software is activated after the device has rebooted.

Table 183: Upload Package Summary

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

Installing Software Upgrades Using the CLI



NOTE: This procedure applies only to upgrading one JUNOS Software (legacy services) release to another or upgrading one JUNOS Software release to another. To upgrade JUNOS Software (legacy services) to JUNOS Software, see the *JUNOS Software Migration Guide*.

To install software upgrades on a device with the CLI:

1. Before installing the software upgrade, verify the available space on the CompactFlash card. For information about verifying available CompactFlash card space, see the *JUNOS Software Release Notes*.
2. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 254.
3. If you are installing the software package from a local directory on the device, copy the software package to the device. We recommend that you copy it to the `/var/tmp` directory.
4. To install the new package on the device, enter the following command in operational mode in the CLI:

```
user@host> request system software add unlink no-copy source
```

Replace *source* with one of the following paths:

- For a software package that is installed from a local directory on the device—*/pathname/package-name* (for example, `/var/tmp/junos-jsr-8.5R1.1.domestic.tgz`)
- For software packages that are downloaded and installed from a remote location:
 - `ftp://hostname/pathname/package-name`
 - or
 - `http://hostname/pathname/package-name`
 - or
 - `tftp://hostname/package-name`

The TFTPBOOT installation method is only supported on the SRX210 and SRX650 Services Gateways. For more information on prerequisites and installation method for TFTP, see “Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway” on page 259.

By default, the `request system software add` 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.

The `unlink` option removes the package at the earliest opportunity so that the device has enough storage capacity to complete the installation.

(Optional) The `no-copy` option specifies that a software package is installed, but a copy of the package is not saved. Include this option if you do not have enough space on the CompactFlash card to perform an upgrade that keeps a copy of the package on the device.

5. After the software package is installed, reboot the device:

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

When the reboot is complete, the device displays the login prompt.

Installing Software using the TFTPBoot Method on the SRX100, SRX210, and SRX650 Services Gateway

You can install the JUNOS Software using the Trivial File Transfer Protocol BOOT (TFTPBOOT) method. The device is shipped with the JUNOS Software loaded on the primary boot device. During install or upgrade of the JUNOS Software, the secondary boot device in the services gateway retrieves the JUNOS Software package from a TFTP server. The software image is then installed on the internal flash.

The TFTPBOOT method of installation can be used:

- To bring up the device if the standard boot process fails.
- To install the JUNOS Software on the device for the first time.
- To boot JUNOS Software without using the internal flash.



NOTE: The TFTPBOOT method can be used only on LANs.

Prerequisites

Before you begin the installation, ensure the following prerequisites are met:

- The device with or without JUNOS Software image.
- The device with U-boot and Loader up and running.
- TFTP server available and loaded with the JUNOS package to be installed on the device.
- TFTP server with Bootstrap Protocol (BOOTP) or DHCP support.

If BOOTP or DHCP support is not available, then you need to configure the gateway IP address, device IP address, and the netmask manually by setting environment variables. For more information, see the “Setting Environment Variables for BOOTP or DHCP Support” on page 260 section.

- Functional network connectivity between the device and the TFTP server.
- Ethernet interface support for the kernel of the device.

This support is required to stream the ISO image from the TFTP server to the device.

Setting Environment Variables for BOOTP or DHCP Support

If the TFTP server does not support BOOTP or DHCP, you need to set the following environmental variables:

```
set gatewayip = gateway IP Address
```

```
set ipaddr = IP Address of the device
```

```
set netmask = netmask
```

```
set serverIP = server IP
```

To set these environment variables, you need to access the U-boot prompt. For more information on accessing this prompt, see “Accessing the U-Boot Prompt” on page 260.

Accessing the Loader Prompt

To access the Loader prompt:

1. Telnet to the device.
2. Reboot the device.

During reboot, the following message is displayed:

```
Loading /boot/defaults/loader.conf
```

After this message appears, you are prompted with:

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

3. Press the space bar to get to the Loader prompt.

The loader> prompt appears.

Accessing the U-Boot Prompt

To access the U-boot prompt:

1. Telnet to the device.
2. Reboot the device.

During reboot, the following messages are displayed:

```
Root Hub 0: 3 USB Device(s) found
```

```
Root Hub 1: 1 USB Device(s) found
```

```
scanning bus for storage devices... 1 Storage Device(s) found
```


After this message appears, you are prompted with:

Press the space bar to abort autoboot in 10 seconds: 0

3. Press any key to stop autoboot.

The => U-boot prompt appears.

Example for Setting Up Environment Variable

This example shows you how to proceed with setting up of environment variables. When you reboot a device, the following messages are displayed.

Follow the instructions to access the U-boot prompt and set environment variables at that prompt.

```
Root Hub 0: 3 USB Device(s) found Root Hub 1: 1 USB Device(s) found
scanning bus for storage devices... 1 Storage Device(s) found
Hit any key to stop autoboot: 0
=>
=> setenv ipaddr 10.157.70.170
=> setenv netmask 255.255.255.0
=> setenv gatewayip 10.157.64.1
=> setenv serverip 10.157.60.1
=> save
```

Installing JUNOS Software Using TFTPBOOT

To install the software image on the internal flash of the device:

1. Go to the Loader prompt. For more information on accessing the Loader prompt, see “Accessing the Loader Prompt” on page 260 section.
2. Enter the following command at the Loader prompt:

```
Loader> install URL
```

Where *URL* is *tftp://host/package*

Example:

```
Loader>install tftp://10.77.25.12/junos-srxsme-9.4-200811.0-domestic.tgz
```

The Loader gets the IP address of the device, the IP address of the TFTP server, the IP address of the gateway, and the netmask.

Using this information, the Loader accesses the JUNOS package on the TFTP server and streams the installation files to the kernel using TFTP. The Loader loads and boots the kernel.

3. The install script available in the installation file executes. This script does the following:
 - Enables the Ethernet interface.
 - Downloads the JUNOS package from the server using TFTP.
 - Installs the package on the internal flash.

After the installation of the software image, the device boots from the internal flash.



CAUTION: When you install the JUNOS image using the TFTP method, the existing configurations, if any, in the device will be erased completely. Therefore we recommend you to backup the configuration files before you plan to install or upgrade the software image on the device.

Downgrading the Software

When you upgrade your software, the device creates a backup image of the software that was previously installed, as well as installs the requested software upgrade.

To downgrade the software, you can use the backup image of the software that was previously installed, which is saved on the device. If you revert to the previous image, this backup image is used, and the image of the running software is deleted. You can downgrade to only the software release that was installed on the device before the current release with this method.

Use the procedures as described in “Installing Software Upgrades with the J-Web Interface” on page 255 and “Installing Software Upgrades Using the CLI” on page 257 and specify an older software image as the source image to be upgraded.

Downgrade your software with either the J-Web interface or the CLI.



NOTE: To downgrade JUNOS Software to JUNOS Software (legacy services), see the *JUNOS Software Migration Guide*.

This section contains the following topics:

- Downgrading the Software with the J-Web Interface on page 262
- Downgrading the Software with the CLI on page 263

Downgrading the Software with the J-Web Interface

You can downgrade the software from the J-Web interface. For your changes to take effect, you must reboot the device.



NOTE: This procedure applies only to downgrading one JUNOS Software release to another or one JUNOS Software services release to another. To downgrade JUNOS Software services to the JUNOS Software, see the *JUNOS Software Migration Guide*.

To downgrade software with the J-Web interface:

1. In the J-Web interface, select **Maintain > Software > Downgrade**. The image of the previous version (if any) is displayed 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. When the downgrade process is complete, for the new software to take effect, click **Maintain > Reboot** from the J-Web interface to reboot the device.

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 of software, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Downgrading the Software with the CLI

You can revert to the previous version of software using the **request system software rollback** command in the CLI. For the changes to take effect, you must reboot the device. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image labeled with the appropriate release.



NOTE: This procedure applies only to downgrading one JUNOS Software release to another or one JUNOS Software services release to another. To downgrade JUNOS Software services to the JUNOS Software, see the *JUNOS Software Migration Guide*.

To downgrade software with the CLI:

1. Enter the **request system software rollback** command to return to the previous JUNOS Software version:

```
user@host> request system software rollback
```

The previous software version is now ready to become active when you next reboot the device.

2. Reboot the device:

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

The device is now running the previous version of the software. To downgrade to an earlier version of software, follow the procedure for upgrading, using the software image labeled with the appropriate release.

Configuring Boot Devices

You can configure a boot device to replace the primary boot device on your J Series or SRX Series device, or to act as a backup boot device. The backup device must have a storage capacity of at least 256 MB. Use either the J-Web 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 or 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 CompactFlash card from a special software image. You can also configure a boot device to store snapshots of software failures, for use in troubleshooting.

For information about installing boot devices, see the *J Series Services Routers Hardware Guide*.

This section contains the following topics:

- Configuring a Boot Device for Backup with the J-Web Interface on page 264
- Configuring a Boot Device for Backup with the CLI on page 266
- Configuring a Boot Device to Receive Software Failure Memory Snapshots on page 268

Configuring a Boot Device for Backup with the J-Web Interface

You can use the J-Web interface to create a boot device on an alternate medium, to replace the primary boot device or serve as a backup.

Figure 10 on page 264 shows the Snapshot page.

Figure 10: Snapshot Page

[Manage](#) > [Snapshot](#)

Snapshot

System Snapshot

You can configure boot devices to replace the primary boot device on your router or to act as a backup boot device. To do this, you create a snapshot of the system software running on your router, 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 compact-flash

Factory ☐

Partition ☐

☐ **Advanced options**

To create a boot device:

1. In the J-Web interface, select **Maintain > Snapshot**.
2. On the Snapshot page, enter information into the fields described in Table 184 on page 265.
3. Click **Snapshot**.
4. Click **OK**.

Table 184: Snapshot Summary

Field	Function	Your Action
Target Media	<p>Specifies the boot device to copy the snapshot to.</p> <p>NOTE: You cannot copy software to the active boot device.</p>	<p>In the list, select a boot device that is not the active boot device:</p> <ul style="list-style-type: none"> ■ compact-flash—Copies software to the internal compact flash. ■ removable-compact-flash—Copies software to the external compact flash. This option is available on J2320 and J2350 Services Routers only. ■ usb—Copies software to the device connected to the USB port.
Factory	<p>Copies 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.</p> <p>NOTE: After a boot device is created with the default factory configuration, it can operate only in an internal compact flash slot.</p>	<p>To copy only the default factory configuration, plus a rescue configuration if one exists, select the check box.</p>
Partition	<p>Partitions the medium. This process is usually necessary for boot devices that do not already have software installed on them.</p>	<p>To partition the medium that you are copying the snapshot to, select the check box.</p>
As Primary Media	<p>On an external compact flash or USB storage device only, creates a snapshot for use as the primary boot medium.</p> <p>Use this feature to replace the medium in the internal compact flash slot or to replicate it for use in another device. This process also partitions the boot medium.</p> <p>NOTE: After the boot device is created as an internal compact flash, it can operate only in an internal compact flash slot.</p>	<p>To create a boot medium to use in the internal compact flash only, select the check box.</p>

Table 184: Snapshot Summary (*continued*)

Field	Function	Your Action
Data Size	<p>Specifies the size of the data partition, in kilobytes.</p> <p>The data partition is mounted on /data. This space is not used by the device, and can be used for extra storage.</p> <p>This selection also partitions the boot medium.</p>	Type a numeric value, in kilobytes. The default value is 0 KB.
Swap Size	<p>Specifies the size of the swap partition, in kilobytes.</p> <p>The 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.</p> <p>For information about the setting the dump device, see “Configuring a Boot Device to Receive Software Failure Memory Snapshots” on page 268.</p> <p>This selection also partitions the boot medium.</p>	Type a numeric value, in kilobytes. The default value is one-third of the physical memory on a boot medium larger than 128,000 KB, or 0 KB on a smaller boot device.
Config Size	<p>Specifies the size of the config partition, in kilobytes.</p> <p>The config partition is mounted on /config. The configuration files are stored in this partition.</p> <p>This selection also partitions the boot medium.</p>	Type a numeric value, in kilobytes. The default value is 10 percent of physical memory on the boot medium.
Root Size	<p>Specifies the size of the root partition, in kilobytes.</p> <p>The root partition is mounted on / and does not include configuration files.</p> <p>This selection also partitions the boot medium.</p>	Type a numeric value, in kilobytes. The default value is the boot device's physical memory minus the config , data , and swap partitions.

Configuring a Boot Device for Backup with the CLI

Use the **request system snapshot** CLI command to create a boot device on an alternate medium, to replace the primary boot device or serve as a backup. Enter the command with the following syntax:

```
user@host> request system snapshot <as-primary> <config-size size> <data-size size> <factory> <media type> <partition> <root-size size> <swap-size size>
```

Table 185 on page 267 describes the **request system snapshot** command options. Default values are in megabytes, but you can alternatively enter values in kilobytes

by appending **k** to the number. For example, **config-size 10** specifies a **config** partition of 10 MB, but **config-size 10k** specifies a **config** partition of 10 KB.

Table 185: CLI request system snapshot Command Options

Option	Description
as-primary	<p>On an external CompactFlash card or USB storage device only, creates a snapshot for use as the primary boot medium.</p> <p>Use the as-primary option to replace the medium in the internal CompactFlash card slot or to replicate it for use in another device. This process also partitions the boot medium.</p> <p>NOTE: After the boot device is created as an internal CompactFlash, it can operate only in an internal CompactFlash slot.</p>
config-size size	<p>Specifies the size of the config partition, in megabytes. The default value is 10 percent of physical memory on the boot medium.</p> <p>The config partition is mounted on /config. The configuration files are stored in this partition.</p> <p>This option also partitions the boot medium.</p>
data-size size	<p>Specifies the size of the data partition, in megabytes. The default value is 0 MB.</p> <p>The data partition is mounted on /data. This space is not used by the device, and can be used for extra storage.</p> <p>This option also partitions the boot medium.</p>
factory	<p>Copies only default files that were loaded on the internal CompactFlash card when it was shipped from the factory, plus the rescue configuration if one has been set.</p> <p>NOTE: After the boot medium is created with the factory option, it can operate in only the internal CompactFlash slot.</p>
media type	<p>Specifies the boot device the software snapshot is copied to:</p> <ul style="list-style-type: none"> ■ compact-flash—Copies software to the internal CompactFlash. ■ removable-compact-flash—Copies software to the external CompactFlash. This option is available on J2320 and J2350 Services Routers only. ■ usb—Copies software to the device connected to the USB port. <p>NOTE: You cannot copy software to the active boot device.</p>
partition	<p>Partitions the medium. This option is usually necessary for boot devices that do not have software already installed on them.</p>
root-size size	<p>Specifies the size of the root partition, in megabytes. The default value is the boot device's physical memory minus the config, data, and swap partitions.</p> <p>The root partition is mounted on / and does not include configuration files.</p> <p>This option also partitions the boot medium.</p>

Table 185: CLI request system snapshot Command Options (*continued*)

Option	Description
swap-size size	<p>Specifies the size of the swap partition, in megabytes. The default value is one-third of the physical memory on a boot medium larger than 128 MB, or 0 MB on a smaller boot device.</p> <p>The 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. For information about the setting the dump device, see “Configuring a Boot Device to Receive Software Failure Memory Snapshots” on page 268.</p> <p>NOTE: This option also partitions the boot medium.</p>

Configuring a Boot Device to Receive Software Failure Memory Snapshots

You can use the **set system dump-device** CLI 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.

Enter the **set system dump-device** CLI command with the following syntax:

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

Table 186 on page 268 describes the **set system dump-device** command options.

Table 186: CLI set system dump-device Command Options

Option	Description
boot-device	Uses whatever device was booted from as the system software failure memory snapshot device.
compact-flash	Uses the internal CompactFlash card as the system software failure memory snapshot device.
removable-compact-flash	Uses the CompactFlash card on the rear of the device (J2320 and J2350 only) as the system software failure memory snapshot device.

Table 186: CLI set system dump-device Command Options (continued)

Option	Description
usb	Uses the device attached to the USB port as the system software failure memory snapshot device.

Rebooting or Halting the Device

Reboot or halt your J Series or SRX Series device with either the J-Web interface or the CLI. This section contains the following topics:

- Rebooting or Halting the Device with the J-Web Interface on page 269
- Rebooting the Device with the CLI on page 271
- Halting the Device with the CLI on page 271

Rebooting or Halting the Device with the J-Web Interface

You can use the J-Web interface to schedule a reboot or halt the J Series or SRX Series device.

Figure 11 on page 269 shows the Reboot page for the device.

Figure 11: Reboot Page

[Manage](#) > [Reboot](#)

Reboot

Schedule Reboot Or Halt

To reboot or halt the system, please select a time below.

Note that a halted system can only be accessed from the system console port.

The current system time is 20:45 (8:45 PM). Reboots scheduled to occur in the future will occur regardless of whether you log out of web management.

☐ Reboot Immediately
☒ Reboot in 5 minutes
☐ Reboot when the system time is 20:50
☐ Halt Immediately

Reboot From Media: compact-flash

Message:

To reboot or halt the device with the J-Web interface:

1. In the J-Web interface, select **Maintain > Reboot**.
2. Select one of the following options:
 - **Reboot Immediately**—Reboots the device immediately.
 - **Reboot in *number of minutes***—Reboots the device in the number of minutes from now that you specify.
 - **Reboot when the system time is *hour:minute***—Reboots the device at the absolute time that you specify, on the current day. You must select a 2-digit hour in 24-hour format, and a 2-digit minute.
 - **Halt Immediately**—Stops the device software immediately. After the software has stopped, you can access the device through the console port only.
3. Choose the boot device from the **Reboot from media** list:
 - **compact-flash**—Reboots from the internal CompactFlash card. This selection is the default choice.
 - **removable-compact-flash**—Reboots from the optional external compact CompactFlash card. This selection is available on J2320 and J2350 Services Routers only.
 - **usb**—Reboots from the USB storage device.
4. (Optional) In the Message box, type a message to be displayed to any users on the device before the reboot occurs.
5. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
6. Click **OK** to confirm the operation.
 - If the reboot is scheduled to occur immediately, the device reboots. You cannot access the J-Web interface 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 interface login page.
 - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
 - If the 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 lights during startup and remains steadily green when the device is operating normally.

Rebooting the Device with the CLI

You can use the `request system reboot` CLI command to schedule a reboot the J Series or SRX Series device:

```
user@host> request system reboot <at time> <in minutes> <media type> <message "text">
```

Table 187 on page 271 describes the `request system reboot` command options.

Table 187: CLI Request System Reboot Command Options

Option	Description
<code>none</code>	Same as <code>at now</code> (reboots the device immediately).
<code>at time</code>	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"> ■ <code>now</code>—Reboots the device immediately. This is the default. ■ <code>+minutes</code>—Reboots the device in the number of minutes from now that you specify. ■ <code>yymmddhhmm</code>—Reboots the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute. ■ <code>hh:mm</code>—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.
<code>in minutes</code>	Specifies the number of minutes from now to reboot the device. This option is a synonym for the <code>at +minutes</code> option.
<code>media type</code>	Specifies the boot device to boot the router from: <ul style="list-style-type: none"> ■ <code>compact-flash</code>—Reboots from the internal CompactFlash card. This is the default. ■ <code>removable-compact-flash</code>—Reboots from the optional external CompactFlash card. This option is available on J2320 and J2350 Services Routers only. ■ <code>usb</code>—Reboots from the USB storage device.
<code>message "text"</code>	Provides a message to display to all system users before the device reboots.

Halting the Device with the CLI

You can use the `request system halt` CLI command to halt the J Series or SRX Series device:

```
user@host> request system halt <at time> <in minutes> <media type> <message "text">
```

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 lights during startup and remains steadily green when the device is operating normally.

Table 188 on page 272 describes the **request system halt** command options.

Table 188: CLI Request System Halt Command Options

Option	Description
none	Same as at now (stops software processes on the device immediately).
at time	Time at which to stop the software processes on the device. You can specify time in one of the following ways: <ul style="list-style-type: none"> ■ now—Stops the software processes immediately. This is the default. ■ +minutes—Stops the software processes in the number of minutes from now that you specify. ■ yymmddhhmm—Stops the software processes at the absolute time you specify. Enter the year, month, day, hour (in 24-hour format), and minute. ■ hh:mm—Stops the software processes at the absolute time that you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
in minutes	Specifies the number of minutes from now to stop the software processes on the device. This option is a synonym for the at +minutes option.
media type	Specifies the boot device to boot the router from after the halt: <ul style="list-style-type: none"> ■ compact-flash—Reboots from the internal CompactFlash card. This is the default. ■ removable-compact-flash—Reboots from the optional external CompactFlash card. This option is available on J2320 and J2350 Services Routers only. ■ usb—Reboots from the USB storage device.
message "text"	Provides a message to display to all system users before the software processes on the device are stopped.

Bringing Chassis Components Online and Offline

You can use the CLI request commands to bring all chassis components (except Power Entry Modules and fans) online and offline.

To bring chassis components online and offline, enter the following from the request chassis CLI command.

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

< fru > in the request chassis command can be any of the following:

- `cb` — This changes the control board status.
- `cluster` — This changes the flexible PIC concentrator status.
- `fabric` — This changes the fabric status.
- `fpc` — This changes the flexible PIC concentrator status.
- `fpm` — This changes the craft interface status.
- `pic` — This changes the physical interface card status.
- `routing-engine` — This changes the routing engine status.

For example, to bring specific pic and corresponding fpc slot online, the CLI request might appear as follows:

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

Chassis Control Restart Options

Using the CLI restart chassis-control commands, you have the following chassis restart options.

- Restart the process gracefully.

```
user@host> restart chassis-control gracefully
```
- Restart the process immediately (SIGKILL).

```
user@host> restart chassis-control immediately
```
- Restart the process softly (SIGHUP).

```
user@host> restart chassis-control soft
```
- Restart the process.

```
user@host> restart chassis-control |
```


Chapter 17

Understanding and Changing Secure and Router Contexts

A J Series Services Router running JUNOS Software includes two configurations that allow the router to operate as either a stateful firewall or a router. When a services router is initially configured as a firewall, it operates in secure context. When a services router is initially configured as a router, it operates in router context. Use either of the configurations as a starting point from which you can customize the configuration for your network requirements.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Understanding Secure and Router Contexts on page 275
- Secure Context Configuration Settings on page 276
- Router Context Configuration Settings on page 279
- Changing from Secure Context to Router Context on page 281
- Changing from Router Context to Secure Context on page 285

Understanding Secure and Router Contexts

As shipped from the factory, a services router running JUNOS Software initially starts up and uses a configuration that places the router in secure context. You can change the context in which the services router is running from secure context to router context. To do so, use a predefined template configuration file. If you plan to use the services router primarily as a router, change to router context, using this configuration as your starting point.



CAUTION: If you plan to change contexts, do so before you configure anything else on the services router. If you change contexts after you have configured the services router, your configuration is overwritten by the default configuration for the new context.

Secure Context

Secure context allows a services router to act as a stateful firewall with only management access. To allow traffic to pass through a services router, you must explicitly configure a security policy for that purpose. In secure context, a services router forwards packets only if a security policy permits it. Certain services are also configured (in the `host-inbound-traffic` statement at the `[edit security zones]` hierarchy level) to allow host-inbound traffic for management of a services router. A services router running in secure context is a secure routing device with predefined configuration values.

For secure context configuration details, see “Secure Context Configuration Settings” on page 276. For information about how to change from router context to secure context, see “Changing from Router Context to Secure Context” on page 285.

Router Context

Router context allows a services router to act as a router, in which all management and transit traffic is allowed. All interfaces are bound to the trust zone, and host inbound traffic from all predefined services is allowed. In router context, the services router forwards all packets unless you configure a security policy that denies specific traffic.

JUNOS Software is a hardened operating system. You can use JUNOS Software with more relaxed checks for host-inbound traffic and configure the dataplane with default transit policies to permit all traffic. In this scenario, the services router operates in a router context.

You load a predefined template configuration, `jsr-series-routermode-factory.conf`, to change to router context. In router context, the services router remains flow-enabled. All security features are available, but they are explicitly denied.

For router context configuration details, see “Router Context Configuration Settings” on page 279. For information about how to change from secure context to router context, see “Changing from Secure Context to Router Context” on page 281.

Secure Context Configuration Settings

The following factory configuration settings are defined for secure context:

- The built-in Gigabit Ethernet interface `ge-0/0/0` is bound to a preconfigured zone called “trust.” All other interfaces are bound to a preconfigured zone named “untrust.”

The `ge-0/0/0` interface is configured to allow management access with SSH and HTTP services enabled. The following host-inbound services are configured for the `ge-0/0/0` interface in the trust zone:

- HTTP
- HTTPS

- SSH
- DHCP
- For the trust zone, TCP reset is enabled. The default policy for the trust zone allows transmission of traffic from the trust zone to the untrust zone. All traffic within the trust zone is allowed.
- A screen is applied to a zone to protect against attacks launched from within the zone. The following screens are enabled for the untrust zone:
 - ICMP ping-of-death
 - IP source route options
 - IP teardrop
 - TCP land attack
 - TCP SYN flood with the following settings:
 - Alarm threshold of 1024 half-complete proxy connections per second
 - Attack threshold of 200 SYN packets per second
 - Source threshold of 1024 SYN segments the router can receive per second
 - Destination threshold of 2048 SYN segments received per second
 - Queue size of 2000 proxy connection requests
 - Timeout of 20 seconds
- The default policy for the untrust zone is to deny all traffic.

Secure context configuration values are defined as follows:

```
system {
  autoinstallation {
    delete-upon-commit;
    traceoptions {
      level verbose;
      flag {
        all;
      }
    }
  }
}
services {
  ssh;
  web-management {
    http {
      interface [ ge-0/0/0.0 ];
    }
  }
}
syslog {
  user * {
```

```

        any emergency;
    }
    file messages {
        any any;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
}
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;
                    queue-size 2000;
                    timeout 20;
                }
                land;
            }
        }
    }
}
zones {
    security-zone trust {
        tcp-rst;
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        http;
                        https;
                        ssh;
                        dhcp;
                    }
                }
            }
        }
    }
}
}
security-zone untrust {

```

```

        screen untrust-screen;
    }
}
policies {
    from-zone trust to-zone trust {
        policy default-permit {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
from-zone trust to-zone untrust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy default-deny {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}
}

```

Router Context Configuration Settings

The following configuration settings are defined for router context:

- All transit traffic security checks are disabled.
- The default policy allows all transit traffic, and all interfaces are bound to the “trust” zone.
- Protocol-aware checks for TCP are not performed.
- IPv6 traffic is forwarded.
- Application Layer Gateway (ALG) processing is not performed.

Configuration values are defined as follows in the `jsr-series-routermode-factory.conf` configuration file:

```

system {
  syslog {
    file messages {
      any any;
    }
  }
  services {
    telnet;
    ssh;
    web-management {
      http {
        interface [ ge-0/0/0.0 ];
      }
    }
  }
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
}
security {
  flow {
    allow-dns-reply;
    tcp-session {
      no-syn-check;
      no-syn-check-in-tunnel;
      no-sequence-check;
    }
  }
  forwarding-options {
    family {
      iso {
        mode flow-based;
      }
      inet6 {
        mode packet-based;
      }
    }
  }
  policies {
    default-policy {
      permit-all;
    }
  }
  zones {
    security-zone trust {
      tcp-rst;
      host-inbound-traffic {

```

```

        system-services {
            any-service;
        }
        protocols {
            all;
        }
    }
    interfaces {
        all;
    }
}
}
alg {
    dns disable;
    ftp disable;
    h323 disable;
    mgcp disable;
    real disable;
    rsh disable;
    rtsp disable;
    sccp disable;
    sip disable;
    sql disable;
    talk disable;
    tftp disable;
    ptp disable;
    msrpc disable;
    sunrpc disable;
}
}

```

Changing from Secure Context to Router Context

To operate a services router running JUNOS Software as a routing device, you can use the `jsr-series-routermode-factory.conf` file that contains router context configuration values as a starting point for configuration. After changing to router context, you can customize the configuration for your network.

Secure-to-Router Context Task Overview

To change from secure context to router context, you perform the following tasks:

- Make a backup of your current configuration file.
- Use the `load override` command to load the configuration file for router context (`jsr-series-routermode-factory.conf`).
- Assign a root password for the router. For security purposes, the `jsr-series-routermode-factory.conf` file does not include a default root password. You need to assign a root password so that you are able to commit configuration changes.
- Optionally, to retain remote IP-based connectivity to the services router after changing to router context, perform the following tasks:

- If you have a static IP address assigned to the **ge-0/0/0** interface and do not want to run autoinstallation, you must remove the **[system autoinstallation]** hierarchy from the configuration. Doing so ensures that the router is not automatically assigned an IP address of **192.168.2.1** if it cannot acquire an IP address using DHCP. You must also configure the static IP address that was previously assigned to the **ge-0/0/0** interface.

For more information about autoinstallation, see “Configuring Autoinstallation” on page 127.

- If you do not have remote access to the console, create a local user account to allow remote access for a non-root user account.
- If you previously configured routing information, use your backup configuration file as a reference to configure the routing information for your network.
- Commit the configuration changes, and make the candidate configuration the running configuration.



CAUTION: If you do not assign an IP address for the **ge-0/0/0** interface, create a local user account, and enter routing information, either from CLI configuration or using DHCP, before you commit the changes, the router is no longer remotely accessible. To manage the router, you must connect a PC or laptop to the physical console, or attach the PC or laptop to a subnet that is directly connected to the **ge-0/0/0** interface, which is assigned an IP address of **192.168.2.1**.

Any configuration changes that you made before you issued the **load override** command are no longer part of the current running configuration.



WARNING: For Chassis Cluster Configured Devices Only –

If you have created a chassis cluster and the fabric interfaces have been configured for that cluster, removing the fabric configuration on either node will cause the redundancy group 0 (RG0) secondary node to move to a disabled state. (Resetting a device to the default router mode configuration removes the fabric configuration settings and thereby causes the RG0 secondary node to move to a disabled state.) When the RG0 secondary is in a disabled state, the cluster is effectively not functioning.

If necessary, to return the services router to the factory default (secure context) configuration, you can press the **RESET CONFIG** button. Keep in mind that pressing the **RESET CONFIG** button for 15 seconds or more deletes all configuration files on the services router, including backup configuration and rescue configuration files. The factory configuration is loaded and committed. For more information about the **RESET CONFIG** button, see the *JUNOS Software Administration Guide*.

Changing to Router Context

To change the router from running in secure context to router context:

1. From configuration mode in the CLI, back up your current configuration file. For example, the following command saves a copy of the configuration to a file named `config_backup` in the home directory of the account you used to log in:

```
user@host# save config_backup
Wrote 127 lines of configuration to 'config_backup'
```

2. Make sure that you are currently at the top level of the configuration mode hierarchy. If you are below the top level, enter `exit` to return to the top level.
3. From the top of the configuration hierarchy, enter the `load override` command.

```
user@host# load override /etc/config/jsr-series-routermode-factory.conf
```

4. Assign a root password for the router:

```
user@host# set system root-authentication plain-text-password
New password:
Retype new password:

[edit]
user@host#
```

The password does not appear as you type.

5. Do one of the following:
 - If you have a static IP assigned to the `ge-0/0/0` interface and do not want to run autoinstallation, go to Step 6.
 - If you want to run autoinstallation, go to Step 9. For more information about autoinstallation, see “Configuring Autoinstallation” on page 127.
6. If you have an IP address assigned to the `ge-0/0/0` interface, follow these steps:
 - a. Delete the `[system autoinstallation]` hierarchy:

```
user@host# delete system autoinstallation
```

- b. Configure the specific IP address for the `ge-0/0/0` interface:

```
user@host# set interfaces ge-0/0/0 unit logical-unit-number family inet
address ip-address
```

Replace the variables as follows:

- *logical-unit-number*—Number of the logical unit. Use a value from 0 through 16,384.

- *ip-address*—IP address for the *ge-0/0/0* interface.

7. If you do not have console access, create a local user account. For example, the following command creates a local user account with a password that is entered as plain text in the CLI and encrypted by JUNOS Software.

```
user@host# set system login user username class class-name authentication
plain-text-password
```

New password: *type password here*

Retype new password: *retype password here*

Replace the variables as follows:

- *username*—Unique name of up to 64 characters that identifies the user. For details, see “User Accounts” on page 46.
 - *class-name*—Login class that defines user access and command privileges. You can define a login class or use the predefined classes. For details, see “Login Classes” on page 47.
8. Using your backup configuration file as a reference, configure routing as appropriate for your network.
 9. Commit the configuration using one of the following methods:
 - Use the **commit** command to commit the configuration immediately.

```
user@host# commit
commit complete
```

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

- If you do not have console access, use the **commit confirmed** command, which, by default, activates the configuration for 10 minutes. This command allows you to verify if the configuration is working correctly. You must confirm the commit by entering **commit** or **commit-check** within 10 minutes; otherwise, the router loads the previous configuration.

```
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#
```

The configuration is now committed, and its configuration values comprise the running configuration.

10. Use the following methods to access the router, depending on the steps you performed:
 - If you performed Steps 1 through 9, the configuration mode prompt returns in the Telnet or SSH session you used to change contexts. Use the CLI or J-Web interface to continue configuring the router. If you cannot remotely

access the router with the session that you were using, connect to the console remotely or directly to the physical console port.

- If you performed Steps 1 through 4 and Step 9 and autoinstallation successfully assigned an IP address, you can connect to the router using Telnet, SSH, or the J-Web interface. If you cannot access the router remotely, connect a PC or laptop to the physical console port.

For information about autoinstallation, see “Configuring Autoinstallation” on page 127. For information about connecting to the console locally or remotely, see the *J Series Services Routers Hardware Guide*.

Changing from Router Context to Secure Context

To change a services router running JUNOS Software from a router to a secure router, use the `load factory-default` configuration command to load the factory configuration. The factory configuration contains the default secure context configuration values. After changing to secure context, you can customize the configuration to suit your network.

Router-to-Secure Context Task Overview

To change from router context to secure context, you perform the following tasks:

- Make a backup of your current configuration file.
- Use the `load factory-default` command to load the factory configuration file for secure context.
- Assign a root password for the router. For security purposes, the factory configuration does not include a default root password. You need to assign a root password so that you are able to commit configuration changes.
- Optionally, if you want to retain remote IP-based connectivity to the services router after changing to router context, perform the following tasks:
 - If you have a static IP address assigned to the `ge-0/0/0` interface and do not want to run autoinstallation, you must remove the `system autoinstallation` hierarchy from the configuration. Doing so ensures that the router is not automatically assigned an IP address of `192.168.2.1` if it cannot acquire an IP address using DHCP. You must also assign the IP address previously used to the `ge-0/0/0` interface.

For more information about autoinstallation, see “Configuring Autoinstallation” on page 127.

- If you do not have remote access to the console, create a local user account to allow remote access for a non-root user account.
- If you previously configured routing information, use your backup configuration file as a reference to configure the routing information for your network.
- Commit the configuration changes, and make the candidate configuration the running configuration.



CAUTION: If you do not assign an IP address for the `ge-0/0/0` interface, create a local user account, and enter routing information, either from CLI configuration or using DHCP, before you commit the changes, the router is no longer remotely accessible. To manage the router, you must connect a PC or laptop to the physical console, or attach the PC or laptop to a subnet that is directly connected to the `ge-0/0/0` interface, which is assigned an IP address of `192.168.2.1`.

Any configuration changes that you made before you issued the `load override` command are no longer part of the current running configuration.



WARNING: For Chassis Cluster Configured Devices Only –

If you have created a chassis cluster and the fabric interfaces have been configured for that cluster, removing the fabric configuration on either node will cause the redundancy group 0 (RG0) secondary node to move to a disabled state. (Resetting a device to the factory default configuration removes the fabric configuration settings and thereby causes the RG0 secondary node to move to a disabled state.) When the RG0 secondary is in a disabled state, the cluster is effectively not functioning.

Alternatively, to return the services router to the factory default (secure context) configuration, you can press the **RESET CONFIG** button. Keep in mind that pressing the **RESET CONFIG** button for 15 seconds or more deletes all configuration files on the services router, including backup configuration and rescue configuration files. The factory configuration is loaded and committed. Using the `load factory-default` command does not delete all configuration files. For more information about the **RESET CONFIG** button, see the *JUNOS Software Administration Guide*.

To change the router from running in router context to secure context:

1. From configuration mode in the CLI, back up your current configuration file. For example, the following command saves a copy of the configuration to a file named `config_backup` in the home directory of the account you used to log in:

```
user@host# save config_backup
Wrote 127 lines of configuration to 'config_backup'
```

2. In configuration mode, enter the `load factory-default` command.

```
user@host# load factory-default
warning: activating factory configuration

[edit]
user@host#
```

3. Assign a root password for the router:

```
user@host# set system root-authentication plain-text-password
New password:
Retype new password:
```

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

The password does not appear as you type.

4. Do one of the following:
 - If you have a static IP assigned to the **ge-0/0/0** interface and do not want to run autoinstallation, go to Step 5.
 - If you want to run autoinstallation, go to Step 8. For more information about autoinstallation, see “Configuring Autoinstallation” on page 127.
5. If you have an IP address assigned to the **ge-0/0/0** interface, follow these steps:
 - a. Delete the **[system autoinstallation]** hierarchy:

```
user@host# delete system autoinstallation
```

- b. Configure the specific IP address for the **ge-0/0/0** interface:

```
user@host# set interfaces ge-0/0/0 unit logical-unit-number family inet  
address IP-address
```

Replace the variables as follows:

- *logical-unit-number*—Number of the logical unit. Use a value from 0 through 16,384.
 - *IP-address*—IP address for the **ge-0/0/0** interface.
6. If you do not have console access, create a local user account. For example, the following command creates a local user account with a password that is entered as plain text in the CLI and is encrypted by JUNOS Software.

```
user@host# set system login user username class class-name authentication  
plain-text-password
```

New password: *type password here*

Retype new password: *retype password here*

Replace the variables as follows:

- *username*—Unique name of up to 64 characters that identifies the user. For details, see “User Accounts” on page 46.
 - *class-name*—Login class that defines user access and command privileges. You can define a login class or use the predefined classes. For details, see “Login Classes” on page 47.
7. Using your backup configuration file as a reference, configure routing as appropriate for your network.
 8. Commit the configuration using one of the following methods:
 - Use the **commit** command to commit the configuration immediately.

```
user@host# commit  
commit complete
```

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

- If you do not have console access, use the **commit confirmed** command, which, by default, activates the configuration for 10 minutes. This command allows you to verify if the configuration is working correctly. You must confirm the commit by entering **commit** or **commit-check** within 10 minutes; otherwise, the router loads the previous configuration.

```
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#
```

The configuration is now committed, and its configuration values comprise the running configuration.

9. Use the following methods to access the router, depending on the steps you performed:
 - If you performed Steps 1 through 8, the configuration mode prompt returns in the SSH session you used to change contexts. Use the CLI or J-Web interface to continue configuring the router. If you cannot remotely access the router with the session that you were using, connect to the console remotely or directly to the physical console port.
 - If you performed Steps 1 through 3 and Step 8, and autoinstallation successfully assigned an IP address, you can connect to the router using SSH or the J-Web interface. If you cannot access the router remotely, connect a PC or laptop to the physical console port.

For information about autoinstallation, see “Configuring Autoinstallation” on page 127. For information about connecting to the CLI locally or remotely, see the *J Series Services Routers Hardware Guide*.

Chapter 18

Configuring Selective Stateless Packet-Based Services

Selective stateless packet-based services allow you to use both flow-based and packet-based forwarding simultaneously on a system. You can selectively direct traffic that requires packet-based, stateless forwarding to avoid stateful flow-based forwarding by using stateless firewall filters (ACLs). The traffic not so directed follows the default flow-based forwarding path. Bypassing flow-based forwarding can be useful for traffic for which you explicitly want to avoid flow session-scaling constraints.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics. For more information about configuring the stateless firewall filters, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

- Understanding Packet-Based and Flow-Based Forwarding on page 289
- Understanding Selective Stateless Packet-Based Services on page 291
- Configuring Selective Stateless Packet-Based Services on page 292
- Example: Configuring Selective Stateless Packet-Based Services—End-to-End Packet-Based on page 294
- Verifying the Selective Stateless Packet-Based Services Configuration—End-to-End Packet-Based on page 298
- Example: Configuring Selective Stateless Packet-Based Services—Packet-Based to Flow-Based on page 303
- Verifying the Selective Stateless Packet-Based Services Configuration—Packet-Based to Flow-Based on page 307

Understanding Packet-Based and Flow-Based Forwarding

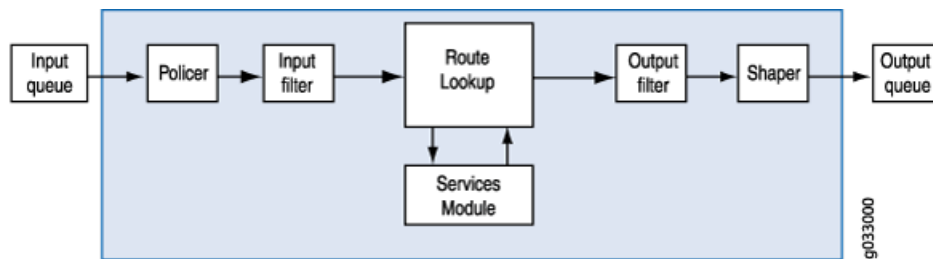
Packets that enter and exit a J Series or SRX Series device running JUNOS Software can undergo packet-based or flow-based processing. Packet-based (stateless) forwarding treats each packet discretely, and flow-based (stateful) packet processing treats related packets, or a stream of packets, in the same way.

Packet-Based Forwarding

Packet-based (stateless) forwarding is performed on a packet-by-packet basis without regard to flow or state information. Each packet is assessed individually for treatment.

Figure 12 on page 290 shows the traffic flow for packet-based forwarding.

Figure 12: Traffic Flow for Packet-Based Forwarding



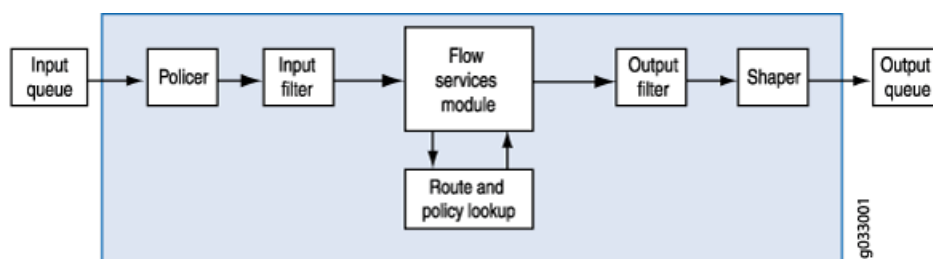
As packets enter the device, classifiers, filters and policers are applied to it. Next, the egress interface for the packet is determined via a route lookup. Once the egress interface for the packet is found, filters are applied and the packet is sent to the egress interface where it is queued and scheduled for transmission.

Packet-based forwarding does not require any information about either previous or subsequent packets that belong to a given connection, and any decision to allow or deny traffic is packet specific. This architecture has the benefit of massive scaling because it forwards packets without keeping track of individual flows or state.

Flow-Based Forwarding

Flow-based (stateful) packet processing requires the creation of sessions. A session is created to store the security measures to be applied to the packets of the flow, to cache information about the state of the flow (for example, logging and counting information), to allocate required resources for the flow for features such as Network Address Translation NAT, and to provide a framework for features such as Application Layer Gateways (ALGs) and firewall features. Figure 13 on page 290 shows traffic flow for flow-based processing.

Figure 13: Traffic Flow for Flow-Based Forwarding



The packet treatment in flow-based forwarding depends on characteristics that were established for the first packet of the packet stream, which is referred to as a flow. To determine if a flow exists for a packet, the system attempts to match the packet's information to that of an existing session based on the following match criteria—source address, destination address, source port, destination port, protocol, and unique session token number for a given zone and virtual router.

Most packet processing occurs in the context of a flow, including management of policies, NAT, zones, most screens, and ALGs.

For an overview of stateless and stateful data processing, see the *JUNOS Software Security Configuration Guide*.

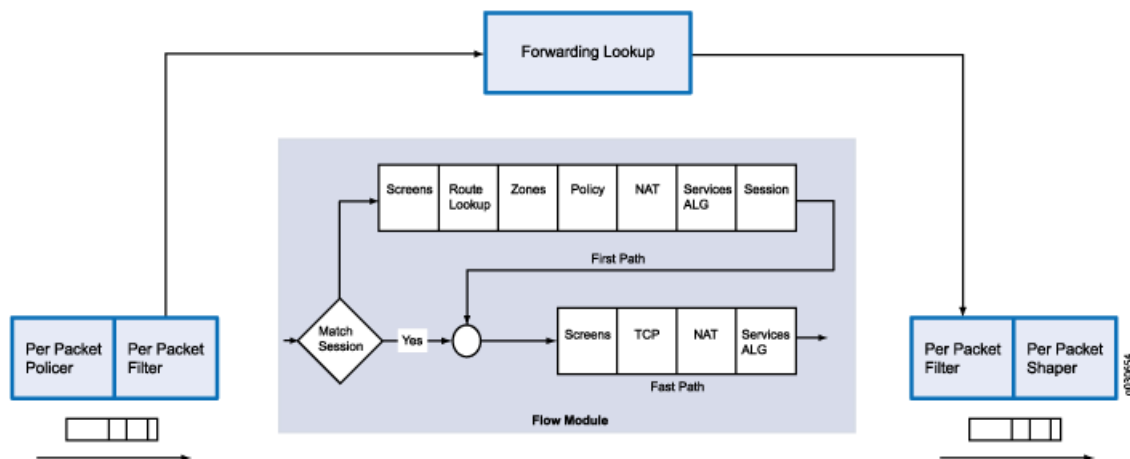
Understanding Selective Stateless Packet-Based Services

By default, J Series and SRX Series devices running JUNOS Software use flow-based forwarding. You can change the context in which your device is running from secure context (using flow-based forwarding) to router context (using packet-based forwarding) by using a predefined template configuration file. Switching between secure and router contexts does allow you both packet-based and flow-based forwarding, but you have to choose one or the other forwarding mode.

Selective stateless packet-based services allow you to have both flow-based and packet-based services simultaneously on a system. This is achieved by configuring stateless firewall filters (ACLs) that allow you to bypass flow-based (stateful) forwarding. Bypassing flow-based forwarding is useful for deployments where you explicitly want to avoid flow session-scaling constraints.

Figure 14 on page 291 shows traffic flow with selective stateless packet-based services bypassing flow-based processing.

Figure 14: Traffic Flow with Selective Stateless Packet-Based Services



When the packet comes in on an interface, the input packet filters configured on the interface are applied.

- If the packet matches the conditions specified in the firewall filter, a **packet-mode** action modifier is set to the packet. The packet-mode action modifier updates a bit field in the packet key buffer—this bit field is used to determine if the flow-based forwarding needs to be bypassed. As a result, the packet with the packet-mode action modifier bypasses the flow-based forwarding completely. The egress interface for the packet is determined via a route lookup. Once the egress interface for the packet is found, filters are applied and the packet is sent to the egress interface where it is queued and scheduled for transmission.
- If the packet does not match the conditions specified in this filter term, it is evaluated against other terms configured in the filter. If, after all terms are evaluated, a packet matches no terms in a filter, the packet is silently discarded. To prevent packets from being discarded, you configure a term in the filter specifying an action to accept all packets.

Packets arriving on interfaces where you have not applied the firewall filter will follow the default flow-based forwarding option.

A defined set of stateless services is available with selective stateless packet-based services:

- IPv4 and IPv6 Routing (unicast and multicast protocols)
- Class of service (CoS)
- Link fragmentation and interleaving (LFI)
- Generic routing encapsulation (GRE)
- Layer 2 Switching
- Multiprotocol Label Switching (MPLS)
- Stateless firewall filters
- Compressed Real-Time Transport Protocol (CRTP)

The following security features are not supported with selective stateless packet-based services—stateful firewall NAT, IPsec VPN, DOS screens, J-flow traffic analysis, WXC integrated security module, security policies, zones, attack detection and prevention, PKI, ALGs, and chassis cluster.

Related Topics

- Understanding Secure and Router Contexts on page 275
- Understanding Packet-Based and Flow-Based Forwarding on page 289

Configuring Selective Stateless Packet-Based Services

Selective stateless packet-based services are configured using the stateless firewall filters (ACLs). You classify traffic for packet-based forwarding by specifying match conditions in the firewall filters and configure a **packet-mode** action modifier to specify

the action. Once match conditions and actions are defined, firewall filters are applied to relevant interfaces.

To configure a firewall filter:

1. Define the address family—First define the address family of the packets that a firewall filter matches. To define the family name, specify **inet** to filter IPv4 packets. Specify **mpls** to filter MPLS packets. Specify **ccc** to filter Layer 2 switching cross-connects.
2. Define terms—Define one or more terms that specify the filtering criteria and the action to take if a match occurs. Each term consists of two components—match conditions and actions.
 - Match conditions—Specify certain characteristics that the packet must match for the action to be performed. You can define various match conditions, such as the IP source address field, IP destination address field, and IP protocol field.
 - Action—Specify what is to be done with the packet if it matches the match conditions. Possible actions are to accept, discard, or reject a packet; go to the next term; or take no action.

You can specify only one **action** statement (or omit it) in a term, but you can specify any combination of action modifiers with it. Action modifiers include a default **accept** action. For example, if you specify an action modifier and do not specify an action, the specified action modifier is implemented and the packet is accepted.

The **packet-mode** action modifier specifies traffic to bypass flow-based forwarding. Like other action modifiers, you can configure the **packet-mode** action modifier along with other actions, such as **accept** or **count**.

3. Apply firewall filters to interfaces—To have the firewall filter take effect, apply it to an interface.

When the packet comes in on an interface, the input packet filters configured on the interface are applied. If the packet matches the specified conditions and **packet-mode** action is configured, the packet bypasses the flow-based forwarding completely.

When configuring filters, be mindful of the order of the terms within the firewall filter. Packets are tested against each term in the order in which it is listed in the configuration. When the first matching conditions are found, the action associated with that term is applied to the packet and the evaluation of the firewall filter ends, unless the **next term** action modifier is included. If the **next term** action is included, the matching packet is then evaluated against the next term in the firewall filter; otherwise, the matching packet is not evaluated against subsequent terms in the firewall filter.

When configuring firewall filters for selective stateless packet-based services:

- Accurately identify traffic that needs to bypass flow to avoid unnecessary packet drops.
- Make sure to apply the firewall filter with packet-mode action on all interfaces involved in the packet-based flow path.

- Make sure to configure host-bound TCP traffic to use flow-based forwarding—exclude this traffic when specifying match conditions for the firewall filter term containing the **packet-mode** action modifier. Any host-bound TCP traffic configured to bypass flow is dropped. Asynchronous flow-mode processing is not supported with selective stateless packet-based services.
- Configure input packet filters (not output) with the **packet-mode** action modifier.



NOTE: Nested firewall filters (configuring a filter within the term of another filter) are not supported with selective stateless packet-based services.

Some typical deployment scenarios where you can configure selective stateless packet-based services are:

- Traffic flow between private LAN and WAN interfaces, such as for Intranet traffic, where end-to-end forwarding is packet-based
- Traffic flow between private LAN and not-so-secure WAN interfaces, where traffic uses packet-based and flow-based forwarding for secure and not so secure traffic respectively
- Traffic flow between the private LAN and WAN interface with failover to flow-based IPsec WAN when the private WAN link is down
- Traffic flow from flow-based LAN to packet-based MPLS WAN

This chapter covers the deployment scenarios for end-to-end packet-based forwarding and traffic flow with packet-based to flow-based forwarding. For information about configuring other deployment scenarios, contact your Juniper channel-partner/value-added-reseller, sales account team or customer support representative, or refer to the *Selective Packet Services App. Note*.

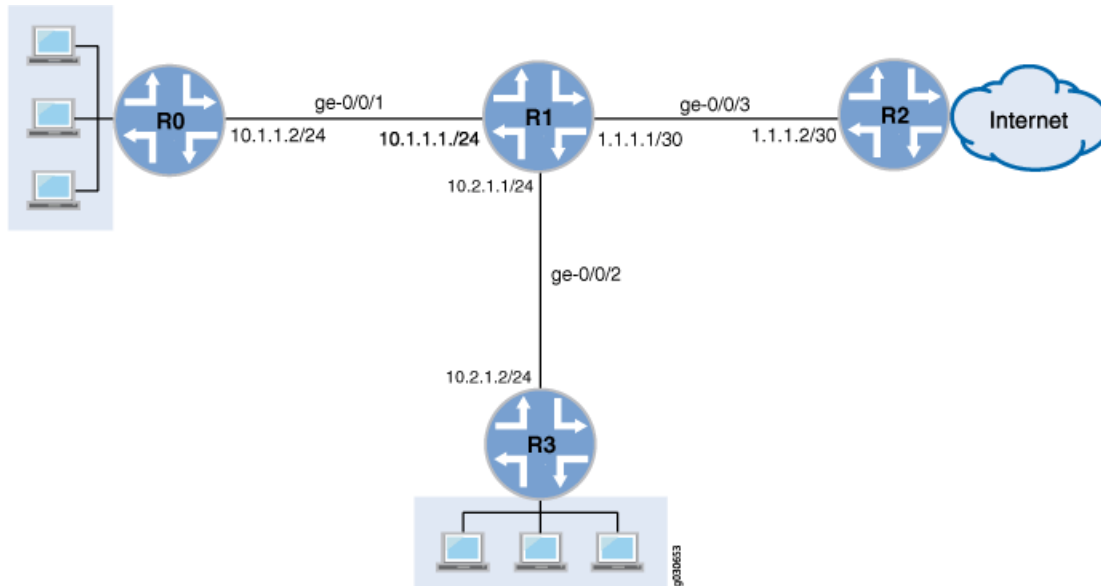
Example: Configuring Selective Stateless Packet-Based Services—End-to-End Packet-Based

In this example, you configure devices for typical Intranet traffic flowing between private WAN interfaces. In this case, end-to-end forwarding is packet-based and the traffic bypasses flow-based forwarding completely.

Before You Begin

1. For background information about configuring stateless firewall filters, see the *JUNOS Software Interfaces and Routing Configuration Guide*.
2. Establish basic connectivity. (See the Getting Started Guide for your device.)

Figure 15 on page 295 shows a network topology that is used in this example.

Figure 15: Intranet Traffic Using End-to-End Packet-Based Services

Your company's branch offices are connected with each other via private WAN. For this internal traffic, packet forwarding is required because security is not an issue. Hence for this traffic, you decide to configure selective stateless packet-based services to bypass flow-based forwarding. The remaining traffic, to and from the Internet, uses flow-based forwarding.

To bypass flow-based processing on Internal traffic, you configure interfaces on devices R0, R1, R2, and R3 used in this configuration. Next, configure the following on device R1:

- Configure zones **trust** and **untrust**. Assign internal interfaces **ge-0/0/1** and **ge-0/0/2** to zone **trust** and interface **ge-0/0/3** to zone **untrust**.
- Configure security policies to allow transit traffic to pass between **trust** and **untrust** zones.
- Create a stateless firewall filter **bypass-flow-filter**. Define two terms—**bypass-flow-term-1** and **bypass-flow-term-2**. Specify source and destination addresses as match conditions and **packet-mode** as the action modifier. Define another term **accept-rest** that does not include the **packet-mode** action modifier.
- Apply the firewall filter **bypass-flow-filter** to interfaces in the internal network—**ge-0/0/1** and **ge-0/0/2**.

In this example, you configure the filter **bypass-flow-filter** with terms **bypass-flow-term-1** and **bypass-flow-term-2** that match the traffic between internal interfaces **ge-0/0/1** and **ge-0/0/2** and contain the **packet-mode** action modifier. You configure the next term **accept-rest** to match the remaining traffic and not contain the **packet-mode** action modifier. Next, you apply this filter on internal interfaces (not on the external interface). As a result, all internal traffic bypasses flow-based forwarding and the traffic to and from the Internet does not bypass flow-based forwarding.

This section includes the following topics:

- CLI Configuration on page 296
- Related Topics on page 298

CLI Configuration

To configure selective stateless packet-based services for end-to-end packet-based forwarding:

1. Configure the IP addresses for the interfaces in your network. In the following statements you configure interfaces on devices R0, R1, R2, and R3:

On device R0:

```
user@R0# set interfaces description "Internal 1" ge-0/0/1 unit 0 family inet
address 10.1.1.2/24
```

On device R1:

```
user@R1# set interfaces description "Internal 1" ge-0/0/1 unit 0 family inet
address 10.1.1.1/24
user@R1# set interfaces description "Internal 2" ge-0/0/2 unit 0 family inet
address 10.2.1.1/24
user@R1# set interfaces description "Internet" ge-0/0/3 unit 0 family inet address
1.1.1.1/30
```

On device R2:

```
user@R2# set interfaces description "Internet" ge-0/0/3 unit 0 family inet address
1.1.1.2/30
```

On device R3:

```
user@R3# set interfaces description "Internal 2" ge-0/0/2 unit 0 family inet
address 10.2.1.2/24
```

2. Create static routes and associate appropriate next-hop addresses. The following statements create static routes and associate next-hop addresses for devices R0, R1, R2, and R3:

On device R0:

```
user@R0# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
```

On device R1:

```
user@R1# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.2
```

On device R2:

```
user@R2# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
```

On device R3:

```
user@R3# set routing-options static route 0.0.0.0/0 next-hop 10.2.1.1
```

3. Configure security zones and assign interfaces to them. In the following statements you create a zone **untrust** and assign interface **ge-0/0/3** to it. You also create a zone **trust** and assign interfaces **ge-0/0/1** and **ge-0/0/2** to it:

```
user@R1# set security zones security-zone untrust interfaces ge-0/0/3
user@R1# set security zones security-zone trust interfaces ge-0/0/1
user@R1# set security zones security-zone trust interfaces ge-0/0/2
```

4. Configure application services for zones. In the following statement you configure **trust** and **untrust** zones to allow all supported application services as inbound services:

```
user@R1# set security zones security-zone trust host-inbound-traffic
system-services all
user@R1# set security zones security-zone untrust host-inbound-traffic
system-services all
```

5. Configure a security policy to allow transit traffic to pass between zones. In the following statements you allow traffic from any source address, destination address, and application to pass between zones:

```
user@R1# set security policies from-zone trust to-zone untrust policy Internet-traffic
match source-address any destination-address any application any
user@R1# set security policies from-zone trust to-zone untrust policy Internet-traffic
then permit
user@R1# set security policies from-zone untrust to-zone trust policy
Incoming-traffic match source-address any destination-address any application
any
user@R1# set security policies from-zone untrust to-zone trust policy
Incoming-traffic then permit
user@R1# set security policies from-zone trust to-zone trust policy Intrazone-traffic
match source-address any destination-address any application any
user@R1# set security policies from-zone trust to-zone trust policy Intrazone-traffic
then permit
```

6. Create a firewall filter and define terms for all the packet-based forwarding traffic. In the following statements you create the firewall filter **bypass-flow-filter**, define the terms **bypass-flow-term-1** and **bypass-flow-term-2**, and specify match conditions and actions for the terms:

```
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-1
from source-address 10.1.1.0/24
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-1
from destination-address 10.2.1.0/24
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-1
then packet-mode
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-2
from source-address 10.2.1.0/24
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-2
from destination-address 10.1.1.0/24
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term-2
then packet-mode
```

7. Define another term for the remaining traffic. In the following statements you define the term `accept-rest` to accept all remaining traffic:

```
user@R1# set firewall family inet filter bypass-flow-filter term accept-rest then
accept
```

8. Apply the firewall filter to relevant interfaces. In the following statements you apply the firewall filter `bypass-flow-filter` to internal interfaces `ge-0/0/1` and `ge-0/0/2`:

```
user@R1# set interfaces description "Internal 1" ge-0/0/1 unit 0 family inet filter
bypass-flow-filter
user@R1# set interfaces description "Internal 2" ge-0/0/2 unit 0 family inet filter
bypass-flow-filter
```

9. If you are finished configuring the router, commit the configuration.

For more information about the configuration statements used in this example, see the *JUNOS Policy Framework Configuration Guide*.

Related Topics

- Verifying the Selective Stateless Packet-Based Services Configuration—End-to-End Packet-Based on page 298
- Configuring Selective Stateless Packet-Based Services on page 292

Verifying the Selective Stateless Packet-Based Services Configuration—End-to-End Packet-Based

To verify selective stateless packet-based services configured in “Example: Configuring Selective Stateless Packet-Based Services—End-to-End Packet-Based” on page 294, perform these tasks:

- Displaying the End-to-End Packet-Based Example Configuration on page 298
- Verifying Session Establishment On Intranet Traffic on page 301
- Verifying Session Establishment On Internet Traffic on page 302

Displaying the End-to-End Packet-Based Example Configuration

Purpose Display the selective stateless packet-based services configuration.

Action From the configuration mode in the CLI, enter the following commands:

- `show interfaces`—Display status information and statistics about interfaces on devices R0, R1, R2, and R3.
- `show routing-options`—Display route information on devices R0, R1, R2, and R3.
- `show security zones`—Display information about security zones on device R1.

- **show security policies**—Display a summary of all security policies configured on device R1.
- **show firewall**—Display firewall filters applied on different interfaces on device R1.

The sample output in this section displays the complete configuration in the example.

On R0:

```
[edit]
user@R0# show interfaces

ge-0/0/1 {
  description "Internal 1"
  unit 0 {
    family inet {
      address 10.1.1.2/24
    }
  }
}

user@R0# show routing-options
static {
  route 0.0.0.0/0 next-hop 10.1.1.1;
}
```

On R2:

```
[edit]
user@R2# show interfaces

ge-0/0/3 {
  description "Internet"
  unit 0 {
    family inet {
      address 1.1.1.2/30;
    }
  }
}

user@R2# show routing-options
static {
  route 0.0.0.0/0 next-hop 1.1.1.1;
}
```

On R3:

```
[edit]
user@R3# show interfaces

ge-0/0/2 {
  description "Internal 2"
  unit 0 {
    family inet {
      address 10.2.1.2/24;
    }
  }
}
```

```

    }
  }
user@R3# show routing-options
static {
  route 0.0.0.0/0 next-hop 10.2.1.1;
}

```

On R1:

```

[edit]
user@R1# show interfaces
ge-0/0/1 {
  description "internal 1"
  unit 0 {
    family inet {
      filter {
        input bypass-flow-filter;
      }
      address 10.1.1.1/24;
    }
  }
}
ge-0/0/2 {
  description "Internal 2"
  unit 0 {
    family inet {
      filter {
        input bypass-flow-filter;
      }
      address 10.2.1.1/24;
    }
  }
}
ge-0/0/3 {
  description "Internet"
  unit 0 {
    family inet {
      address 1.1.1.1/30;
    }
  }
}
user@R1# show routing-options
static {
  route 0.0.0.0/0 next-hop 1.1.1.2;
}
user@R1# show firewall
family inet {
  filter bypass-flow-filter {
    term bypass-flow-term-1 {
      from {
        source-address {
          10.1.1.0/24;
        }
        destination-address {
          10.2.1.0/24;
        }
      }
    }
  }
}

```



```

    }
    then packet-mode;
  }
  term bypass-flow-term-2 {
    from {
      source-address {
        10.2.1.0/24;
      }
      destination-address {
        10.1.1.0/24;
      }
    }
    then packet-mode;
  }
  term accept-rest {
    then accept;
  }
}

```

Meaning Verify that the output shows the intended configuration of the firewall filter, interfaces, and policies.

Verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the `insert` CLI command.

Related Topics For a complete description of `show interfaces` command output, see the *JUNOS Interfaces Command Reference*.

For a complete description of `show security zones` and `show security policies` command outputs, see the *JUNOS Software CLI Reference*.

For a complete description of `show firewall` command output, see the *JUNOS Routing Protocols and Policies Command Reference*.

Verifying Session Establishment On Intranet Traffic

Purpose Verify if, in this example configuration, sessions are established when traffic is transmitted to interfaces within the Intranet.

Action To verify if selective stateless packet-based services are working, you check if Intranet traffic bypasses flow-based forwarding and no sessions are established. To verify if sessions are established, you perform the following tasks:

1. On device **R1**, enter the operational mode command `clear security flow session all` in the CLI to clear all existing security flow sessions.
2. On device **R0**, enter the operational mode command `ping` in the CLI to transmit traffic to device **R3**.
3. On device **R1**, with traffic transmitting from devices **R0** to **R3** through **R1**, enter the operational mode command `show security flow session` in the CLI.



NOTE: To verify established sessions, make sure to enter the `show security flow session` command while the `ping` command is sending and receiving packets.

Sample Output

```
user@R0> ping 10.2.1.2
PING 10.2.1.2 (10.2.1.2): 56 data bytes
64 bytes from 10.2.1.2: icmp_seq=0 ttl=63 time=2.208 ms
64 bytes from 10.2.1.2: icmp_seq=1 ttl=63 time=2.568 ms
64 bytes from 10.2.1.2: icmp_seq=2 ttl=63 time=2.573 ms
64 bytes from 10.2.1.2: icmp_seq=3 ttl=63 time=2.310 ms
64 bytes from 10.2.1.2: icmp_seq=4 ttl=63 time=1.566 ms
64 bytes from 10.2.1.2: icmp_seq=5 ttl=63 time=1.569 ms
...

user@R1>show security flow session
0 sessions displayed
```

Meaning The output shows traffic transmitting from R0 to R3 and no sessions are established. In this example, you applied the `bypass-flow-filter` with the `packet-mode` action modifier on interfaces `Internal 1` and `Internal 2` for your company's Intranet traffic. This output verifies that the traffic between the two interfaces is correctly bypassing flow-based forwarding and hence no sessions are established.

Related Topics For more information about the `show security flow session` command, see the *JUNOS Software CLI Reference*.

For information about the `ping` command, see the *JUNOS Software Administration Guide* or the *JUNOS System Basics Configuration Guide*.

Verifying Session Establishment On Internet Traffic

Purpose Verify if in this example configuration, sessions are established when traffic is transmitted to the Internet.

Action To verify if traffic to the Internet is using flow-based forwarding and sessions are established, perform the following tasks:

1. On device R1, enter the operational mode command `clear security flow session all` in the CLI to clear all existing security flow sessions.
2. On device R0, enter the operational mode command `ping` in the CLI to transmit traffic to device R2.
3. On device R1, with traffic transmitting from R0 to R2 through R1, enter the operational mode command `show security flow session` in the CLI.



NOTE: To verify established sessions, make sure to enter the `show security flow session` command while the `ping` command is sending and receiving packets.

Sample Output

```
user@R0> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
64 bytes from 1.1.1.2: icmp_seq=0 ttl=63 time=2.326 ms
64 bytes from 1.1.1.2: icmp_seq=1 ttl=63 time=2.569 ms
```

```

64 bytes from 1.1.1.2: icmp_seq=2 ttl=63 time=2.565 ms
64 bytes from 1.1.1.2: icmp_seq=3 ttl=63 time=2.563 ms
64 bytes from 1.1.1.2: icmp_seq=4 ttl=63 time=2.306 ms
64 bytes from 1.1.1.2: icmp_seq=5 ttl=63 time=2.560 ms
64 bytes from 1.1.1.2: icmp_seq=6 ttl=63 time=4.130 ms
64 bytes from 1.1.1.2: icmp_seq=7 ttl=63 time=2.316 ms
...

user@R1>show security flow session
Session ID: 50522, Policy name: Internet-traffic/4, Timeout: 2
  In: 10.1.1.2/12 --> 1.1.1.2/2827;icmp, If: ge-0/0/1.0
  Out: 1.1.1.2/2827 --> 10.1.1.2/12;icmp, If: ge-0/0/3.0

Session ID: 50523, Policy name: Internet-traffic/4, Timeout: 2
  In: 10.1.1.2/13 --> 1.1.1.2/2827;icmp, If: ge-0/0/1.0
  Out: 1.1.1.2/2827 --> 10.1.1.2/13;icmp, If: ge-0/0/3.0

2 sessions displayed

```

Meaning The output shows traffic transmitting from devices R0 to R1 and established sessions. In this example, you did not apply the `bypass-flow-filter` with the `packet-mode` action modifier on interface `Internet` for your company's Internet traffic. This output verifies that the traffic to the Internet is correctly using flow-based forwarding and hence sessions are established.

Transmit traffic from device R3 to R2 and use the commands in this section to verify established sessions.

Related Topics For more information about the `show security flow session` command, see the *JUNOS Software CLI Reference*.

For information about the `ping` command, see the *JUNOS Software Administration Guide* or the *JUNOS System Basics Configuration Guide*.

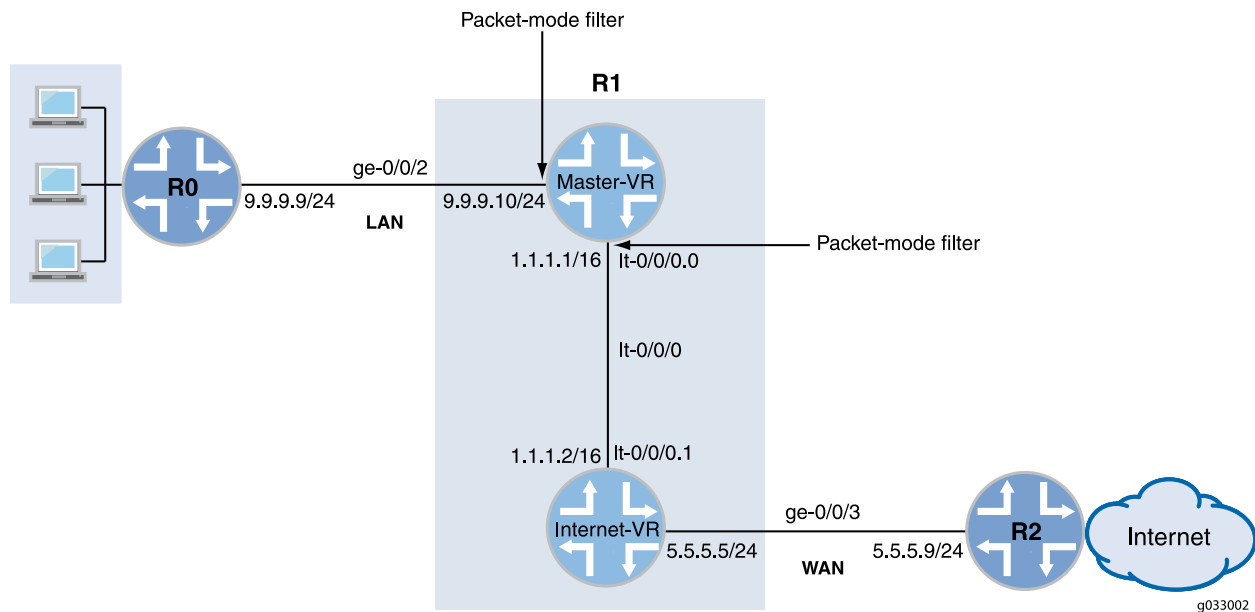
Example: Configuring Selective Stateless Packet-Based Services—Packet-Based to Flow-Based

In this example, you configure devices to direct traffic to use packet-based forwarding on the internal LAN and then direct the same traffic to use flow-based forwarding as it transits to the Internet.

Before You Begin

1. For background information about configuring stateless firewall filters, see the *JUNOS Software Interfaces and Routing Configuration Guide*.
2. Establish basic connectivity. (See the Getting Started Guide for your device.)

Figure 16 on page 304 shows a network topology that is used in this example.

Figure 16: Selective Stateless Packet-Based Services—Packet-Based to Flow-Based

In this example, the interface facing the private LAN does not need any security services, but the interface facing the WAN needs security. In this case, you decide to configure both packet-based and flow-based forwarding for secure and not so secure traffic by configuring two routing instances—one handling the packet-based forwarding and the other handling the flow-based forwarding.

In this example, you create a virtual routing instance to perform flow-based forwarding. The default master routing instance is used to perform packet-based forwarding. You then configure an internal service interface lt-0/0/0 to transmit traffic between the two virtual router routing instances and configure OSPF to exchange the routes between the routing instances. Because all packets traversing the master routing instance need packet-based forwarding, you apply the stateless firewall filter with the **packet-mode** action modifier on all the interfaces (ge-0/0/2 and lt-0/0/0.0) associated with the master routing instance. Similarly, because all packets traversing the virtual routing instance Internet-VR need flow-based forwarding, you do not apply the stateless firewall filter with packet-mode action modifier to all interfaces (ge-0/0/3 and lt-0/0/0.1) associated with this virtual router routing instance.

To bypass flow-based processing on internal traffic, you configure interfaces on devices R0, R1, and R2 used in this configuration. Next, configure the following on device R1:

- Create a virtual router routing instance, **Internet-VR**, allowing you to segment your network to isolate traffic for packet-based and flow-based forwarding on R1.
- Set an internal service interface **lt-0/0/0** to transmit traffic between the two virtual routers.
- Enable OSPF on all interfaces by creating an OSPF area and adding interfaces to it.

- Configure zones and policies to permit all traffic.
- Create a stateless firewall filter **bypass-flow-filter**. Define a term, **bypass-flow-term**, that specifies the action **accept** and the action modifier **packet-mode**.
- Apply the firewall filter **bypass-flow-filter** to interfaces in the internal network—**ge-0/0/2** and **lt-0/0/0.0**.

In this example, you configure the filter **bypass-flow-filter** with the term **bypass-flow-term** that contains the **packet-mode** action modifier. Because you have not specified any match conditions, this filter applies to all traffic that traverses the interfaces on which it is applied. Next, you apply this filter on interfaces associated with the master routing instance. You do not apply the filter to the interfaces associated with the **Internet-VR** routing instance. As a result, all traffic when traversing the LAN interfaces associated with the master routing instance uses packet-based forwarding and when traversing the **Internet-VR** routing instance uses flow-based forwarding.

This section includes the following topics:

- CLI Configuration on page 305
- Related Topics on page 307

CLI Configuration

To configure selective stateless packet-based services for end-to-end packet-based forwarding:

1. Configure the IP addresses for the interfaces in your network. In the following statements you configure interfaces on devices **R0**, **R1**, and **R2**:

On device **R0**:

```
user@R0# set interfaces description "Connect to Master VR" ge-0/0/2 unit 0
family inet address 9.9.9.9/24
```

On device **R1**:

```
user@R1# set interfaces description "Connect to R0" ge-0/0/2 unit 0 family inet
address 9.9.9.10/24
user@R1# set interfaces description "Connect to R2" ge-0/0/3 unit 0 family inet
address 5.5.5.5/24
```

On device **R2**:

```
user@R2# set interfaces description "Connect to Internet-VR" ge-0/0/3 unit 0
family inet address 5.5.5.9/24
```

2. Set an internal service interface **lt-0/0/0** between routing instances. The following statements configure the **lt** service interface and configure a peer relationship between the two virtual routers:

```
user@R1# set interfaces lt-0/0/0 unit 0 encapsulation frame-relay dlci 100
peer-unit 1 family inet address 1.1.1.1/16
user@R1# set interfaces lt-0/0/0 unit 1 encapsulation frame-relay dlci 100
peer-unit 0 family inet address 1.1.1.2/16
```

3. Configure security zones, assign interfaces to zones and configure zones to allow application services and protocols. In the following statements you create a zone **HOST**, assign interfaces to it and configure it, to allow all supported applications and protocols:

```
user@R1# set security zones security-zone HOST host-inbound-traffic
system-services any-service
user@R1# set security zones security-zone HOST host-inbound-traffic protocols
all
user@R1# set security zones security-zone HOST interfaces all
```

4. Configure policies. In the following statement you set the default policy and specify that all packets are permitted:

```
user@R1# set security policies default-policy permit-all
```

5. Configure a virtual router routing instance. The following statement configures a virtual router routing instance **Internet-VR** and assigns interfaces for flow-based forwarding:

```
user@R1# set routing-instances Internet-VR instance-type virtual-router interface
lt-0/0/0.1
user@R1# set routing-instances Internet-VR instance-type virtual-router interface
ge-0/0/3.0
```

6. Enable OSPF on all interfaces in the network. The following statements enable OSPF on devices **R0**, **R1**, and **R2**:

On device **R0**:

```
user@R0# set protocols ospf area 0.0.0.0 interface ge-0/0/2.0
```

On device **R1** (for **Master-VR**):

```
user@R1# set protocols ospf area 0.0.0.0 interface ge-0/0/2.0
user@R1# set protocols ospf area 0.0.0.0 interface lt-0/0/0.0
```

On device **R1** (for **Internet-VR**):

```
user@R1# set routing-instances Internet-VR protocols ospf area 0.0.0.0 interface
lt-0/0/0.1
user@R1# set routing-instances Internet-VR protocols ospf area 0.0.0.0 interface
ge-0/0/3.0
```

On device **R2**:

```
user@R2# set protocols ospf area 0.0.0.0 interface ge-0/0/3
```

7. Create a firewall filter and define a term for packet-based forwarding traffic. In the following statements you create a firewall filter **bypass-flow-filter**, define a term **bypass-flow-term**, and specify actions for the term:

```
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term
then accept
user@R1# set firewall family inet filter bypass-flow-filter term bypass-flow-term
then packet-mode
```

8. Apply the firewall filter to relevant interfaces. In the following statements you apply the firewall filter `bypass-flow-filter` to internal interfaces `ge-0/0/2` and `lt-0/0/0.0`:

```
user@R1# set interfaces ge-0/0/2 unit 0 family inet bypass-flow-filter
user@R1# set interfaces lt-0/0/0 unit 0 family inet bypass-flow-filter
```

9. If you are finished configuring the router, commit the configuration.

For more information about the configuration statements used in this example, see the *JUNOS Software CLI Reference*.

Related Topics

- Verifying the Selective Stateless Packet-Based Services Configuration—End-to-End Packet-Based on page 298
- Configuring Selective Stateless Packet-Based Services on page 292

Verifying the Selective Stateless Packet-Based Services Configuration—Packet-Based to Flow-Based

To verify selective stateless packet-based services configured in “Example: Configuring Selective Stateless Packet-Based Services—Packet-Based to Flow-Based” on page 303, perform these tasks:

- Displaying the Packet-Based to Flow-Based Example Configuration on page 307
- Verifying Session Establishment On LAN Traffic on page 310
- Verifying Session Establishment On Internet Traffic on page 311

Displaying the Packet-Based to Flow-Based Example Configuration

Purpose Display the selective stateless packet-based services configuration for packet-based to flow-based forwarding.

Action From the configuration mode in the CLI, enter the following commands:

- `show interfaces`—Display status information and statistics about interfaces on devices R0, R1, and R2.
- `show protocols`—Display protocol information on devices R0, R1, and R2.
- `show security`—Display information about security zones and policies on device R1.
- `show routing-instances`—Display virtual routing instances configured on device R1.
- `show firewall`—Display firewall filters applied on different interfaces on device R1.

The sample output in this section displays the complete configuration in the example.

On R0:

```
[edit]
user@R0# show interfaces

ge-0/0/2 {
  description "Connect to Master-VR"
  unit 0 {
    family inet {
      address 9.9.9.9/24
    }
  }
}

user@R0# show protocols
ospf {
  area 0.0.0.0/0 {
    interface ge-0/0/2.0;
  }
}
```

On R2:

```
[edit]
user@R2# show interfaces
ge-0/0/3 {
  description "Connect to Internet-VR"
  unit 0 {
    family inet {
      address 5.5.5.9/24;
    }
  }
}

user@R2# show protocols
ospf {
  area 0.0.0.0/0 {
    interface ge-0/0/3.0;
  }
}
```

On R1:

```
[edit]
user@R1# show interfaces
ge-0/0/2 {
  description "Connect to R0"
  unit 0 {
    family inet {
      filter {
        input bypass-flow-filter;
      }
      address 9.9.9.10/24;
    }
  }
}
```



```

lt-0/0/0 {
  unit 0 {
    encapsulation frame-relay;
    dlci 100;
    peer-unit 1;
    family inet {
      filter {
        input bypass-flow-filter
      }
      address 1.1.1.1/16;
    }
  }
  unit 1 {
    encapsulation frame-relay;
    dlci 100;
    peer-unit 0;
    family inet {
      address 1.1.1.2/16;
    }
  }
}
user@R1# show protocols
ospf {
  area 0.0.0.0/0 {
    interface ge-0/0/2.0;
    interface lt-0/0/0.0;
  }
}
user@R1# show firewall
filter bypass-flow-filter {
  term bypass-flow-term {
    then {
      packet-mode;
      accept;
    }
  }
}
user@R1# show routing-instances
Internet-VR {
  instance-type virtual-router;
  interface lt-0/0/0.1;
  interface ge-0/0/3.0;
  protocols {
    ospf {
      area 0.0.0.0 {
        interface ge-0/0/3.0;
        lt-0/0/0.1;
      }
    }
  }
}
user@R1# show security
zones {
  security-zone HOST {

```

```

host-inbound-traffic {
  system-services {
    any-service;
  }
  protocols {
    all;
  }
}
interfaces {
  all;
}
}
}
policies {
  default-policy {
    permit-all;
  }
}
}

```

Meaning Verify that the output shows the intended configuration of the firewall filter, routing instances, interfaces, and policies.

Verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the **insert** CLI command.

Related Topics For a complete description of **show interfaces** command output, see the *JUNOS Interfaces Command Reference*.

For a complete description of **show security zones** and **show security policies** command outputs, see the *JUNOS Software CLI Reference*.

For a complete description of **show firewall** command output, see the *JUNOS Routing Protocols and Policies Command Reference*.

Verifying Session Establishment On LAN Traffic

Purpose Verify if, in this example configuration, sessions are established when traffic is transmitted on interfaces with the firewall filter **bypass-flow-filter**.

Action To verify if selective stateless packet-based services are working, you check if internal traffic bypasses flow-based forwarding and no sessions are established. To verify if sessions are established, you perform the following tasks:

1. On device **R1**, enter the operational mode command **clear security flow session all** in the CLI to clear all existing security flow sessions.
2. On device **R0**, enter the operational mode command **ping** in the CLI to transmit traffic to device **Master-VR**.
3. On device **R1**, with traffic transmitting from devices **R0** through **R1**, enter the operational mode command **show security flow session** in the CLI.



NOTE: To verify established sessions, make sure to enter the `show security flow session` command while the `ping` command is sending and receiving packets.

Sample Output

```
user@R0> ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=63 time=2.208 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=63 time=2.568 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=63 time=2.573 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=63 time=2.310 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=63 time=1.566 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=63 time=1.569 ms
...

user@R1>show security flow session
0 sessions displayed
```

Meaning The output shows traffic transmitting from R0 to Master-VR and no sessions are established. In this example, you applied the `bypass-flow-filter` with the `packet-mode` action modifier on interfaces `ge-0/0/0` and `lt-0/0/0.0` for your company's LAN traffic. This output verifies that the traffic between the two interfaces is correctly bypassing flow-based forwarding and hence no sessions are established.

Related Topics For more information about the `show security flow session` command, see the *JUNOS Software CLI Reference*.

For information about the `ping` command, see the *JUNOS Software Administration Guide* or the *JUNOS System Basics Configuration Guide*.

Verifying Session Establishment On Internet Traffic

Purpose Verify if in this example configuration, sessions are established when traffic is transmitted to the Internet.

Action To verify if traffic to the Internet is using flow-based forwarding and sessions are established, perform the following tasks:

1. On device R1, enter the operational mode command `clear security flow session all` in the CLI to clear all existing security flow sessions.
2. On device R0, enter the operational mode command `ping` in the CLI to transmit traffic to device R2.
3. On device R1, with traffic transmitting from R0 to R2 through R1, enter the operational mode command `show security flow session` in the CLI.



NOTE: To verify established sessions, make sure to enter the `show security flow session` command while the `ping` command is sending and receiving packets.

Sample Output

```
user@R0> ping 5.5.5.9
PING 5.5.5.9 (5.5.5.9): 56 data bytes

64 bytes from 5.5.5.9: icmp_seq=0 ttl=62 time=2.593 ms
```

```

64 bytes from 5.5.5.9: icmp_seq=1 ttl=62 time=2.562 ms
64 bytes from 5.5.5.9: icmp_seq=2 ttl=62 time=2.563 ms
64 bytes from 5.5.5.9: icmp_seq=3 ttl=62 time=2.561 ms
64 bytes from 5.5.5.9: icmp_seq=4 ttl=62 time=2.310 ms
64 bytes from 5.5.5.9: icmp_seq=5 ttl=62 time=3.880 ms

...

user@R1>show security flow session
Session ID: 189900, Policy name: default-policy/2, Timeout: 2
  In: 9.9.9.9/0 --> 5.5.5.9/5924;icmp, If: lt-0/0/0.1
  Out: 5.5.5.9/5924 --> 9.9.9.9/0;icmp, If: ge-0/0/3.0

Session ID: 189901, Policy name: default-policy/2, Timeout: 2
  In: 9.9.9.9/1 --> 5.5.5.9/5924;icmp, If: lt-0/0/0.1
  Out: 5.5.5.9/5924 --> 9.9.9.9/1;icmp, If: ge-0/0/3.0

Session ID: 189902, Policy name: default-policy/2, Timeout: 4
  In: 9.9.9.9/2 --> 5.5.5.9/5924;icmp, If: lt-0/0/0.1
  Out: 5.5.5.9/5924 --> 9.9.9.9/2;icmp, If: ge-0/0/3.0

3 sessions displayed

```

Meaning The output shows traffic transmitting from devices **R0** to **R2** and established sessions. In this example, you did not apply the **bypass-flow-filter** with the **packet-mode** action modifier on routing instance **Internet-VR** for your company's Internet traffic. This output verifies that the traffic to the Internet is correctly using flow-based forwarding and hence sessions are established.

Note that sessions are established only when traffic is flowing between **lt-0/0/0.1** and **ge-0/0/3** and not when traffic is flowing between **ge-0/0/2** and **lt-0/0/0.0**.

Related Topics For more information about the **show security flow session** command, see the *JUNOS Software CLI Reference*.

For information about the **ping** command, see the *JUNOS Software Administration Guide* or the *JUNOS System Basics Configuration Guide*.

Chapter 19

Installing and Managing Licenses

To enable some JUNOS Software 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.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics:

- JUNOS Software Services License Overview on page 313
- Generating a License Key on page 315
- Managing JUNOS Software Services Licenses with the CLI on page 315
- Managing JUNOS Software Services Licenses with the J-Web Interface on page 317
- Verifying JUNOS Software Services License Management on page 319

JUNOS Software Services License Overview

Certain JUNOS Software 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 313
- Software Feature Licenses on page 314
- License Key Components on page 314

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.

Software Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one device. Table 189 on page 314 describes the JUNOS Software features that require licenses.

Table 189: JUNOS Software Services Feature Licenses

JUNOS Software License Requirements						Device	
Feature	J Series	SRX100	SRX210	SRX240	SRX650	SRX3000 line	SRX5000 line
Access Manager			X	X			
BGP Route Reflectors	X		X	X	X		
IDP Signature Update	X		X *	X *	X	X	X
Juniper-Kaspersky Anti-Virus	X	X	X	X	X		
Juniper-Symantec Anti-Spam	X	X	X	X	X		
Juniper-WebSense Integrated Web Filtering	X	X	X	X	X		
SRX100 Memory Upgrade		X					
UTM	X		X *	X *	X		

* Indicates support on high-memory devices only

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 **li29183743** is the license ID, and the trailing block of data is the license data:

```
li29183743 4ky27y acasck 82fsj6 jzsn4q ix8i8d adj7kr
      8uq38t ix8i8d jzsn4q ix8i8d 4ky27y acasck
      82fsj6 ii8i7e adj7kr 8uq38t ks2923 a9382e
```

The license data defines the device ID for which the license is valid and the version of the license.

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 Web page and click **Generate**. Depending on the type of license you purchased, you will receive one of the following:
 - 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 in order 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.

Managing JUNOS Software Services Licenses with the CLI

To manage JUNOS Software licenses with the CLI, perform the following tasks:

- Adding New Licenses with the CLI on page 315
- Deleting a License with the CLI on page 316
- Updating New Licenses with the CLI on page 316
- Saving License Keys with the CLI on page 317

Adding New Licenses with the CLI

To add a new license key to the device with the CLI:

1. Enter operational mode in the CLI.
2. Enter one of the following CLI commands:
 - To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

request system license add *filename* | *url*

Use the *filename* option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.)

Use the *url* option 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.

- To add a license key from the terminal, enter the following command:

request system license add terminal

3. 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.

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

4. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Deleting a License with the CLI

To delete a license key from the device with the CLI:

1. Enter operational mode in the CLI.
2. Enter the following command for each license, specifying the license ID. You can delete only one license at a time.

request system license delete *license-id*

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

3. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Updating New Licenses with the CLI

To update a license key from the device with the CLI:

1. Enter operational mode in the CLI.
2. Enter one of the following CLI commands:
 - To automatically update the license keys, enter the following command:

request system license update url

You can only use this command to update subscription-based licenses (such as UTM).

- To automatically update the trial license keys, enter the following command:

request system license update trial



NOTE: If the URL is not specified, by default the device sends the command to the Juniper Networks LMS server site.

3. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Saving License Keys with the CLI

To save the licenses installed on the device to a file with the CLI:

1. Enter operational mode in the CLI.
2. To save the installed license keys to a file or URL, enter the following command:

```
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
```

3. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Managing JUNOS Software Services Licenses with the J-Web Interface

To manage licenses with the J-Web interface, you perform the following tasks:

- Adding New Licenses with the J-Web Interface on page 318
- Deleting Licenses with the J-Web Interface on page 319
- Displaying License Keys with the J-Web interface on page 319
- Downloading Licenses with the J-Web Interface on page 319

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 190 on page 317.

Table 190: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	<p>Name of the licensed feature:</p> <ul style="list-style-type: none"> ■ Features—Software feature licenses listed in “Software Feature Licenses” on page 314 ■ All features—All-inclusive licenses
Licenses Used	Number of licenses currently being used on the device. Usage is determined by the configuration on the device. If a feature license exists and that feature is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the device for the particular feature.

Table 190: Summary of License Management Fields (*continued*)

Field Name	Definition
Licenses Needed	Number of licenses required for legal use of the feature. Usage is determined by the configuration on the device: If a feature is configured and the license for that feature is not installed, a single license is needed.
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	Valid—The installed license key is valid.
	Invalid—The installed license key is not valid.
Version	Numeric version number of the license key.
Group	If the license defines a group license, this field displays the group definition.
	If the license requires a group license, this field displays the required group definition.
	NOTE: Because group licenses are currently unsupported, this field is always blank.
Enabled Features	Name of the feature that is enabled with the particular license.
Expiry	Verify tha the expiration information for the license is correct.
	For JUNOS Software, only permanent licenses are supported. If a license has expired, it is shown as invalid.

Adding New Licenses with the J-Web Interface

To add a new license key with the J-Web license manager:

1. In the J-Web 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. Use this option 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 the License Key Text box, paste the license key text, in plain-text format, for the license to be added. Use this option to activate a perpetual license directly on the device. (Most feature licenses are perpetual.)
4. Click **OK** to add the license key.

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

5. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Deleting Licenses with the J-Web Interface

To delete one or more license keys with the J-Web license manager:

1. In the J-Web interface, select **Maintain > Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.

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

4. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Displaying License Keys with the J-Web interface

To display the license keys installed on the device with the J-Web license manager:

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.

3. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Downloading Licenses with the J-Web Interface

To download the license keys installed on the device with the J-Web license manager:

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.
4. Go on to “Verifying JUNOS Software Services License Management” on page 319.

Verifying JUNOS Software Services License Management

To verify license management, perform the tasks explained in these sections:

- Displaying Installed Licenses on page 320
- Displaying License Usage on page 320
- Displaying Installed License Keys on page 321

Displaying Installed Licenses

Purpose Verify that the expected licenses are installed and active on the device.

Action From the CLI, enter the `show system license` command.

Sample Output

```
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

```

Meaning The output shows a list of the license usage and a list of the licenses installed on the device and when they expire. Verify the following information:

- Each license is present. Licenses are listed in ascending alphanumeric order by license ID.
- The feature for each license is the expected feature. The features enabled are listed by license. An all-inclusive license has **All features** listed.
- All configured features have the required licenses installed. The **Licenses needed** column must show that no licenses are required.
- The expiration information for the license is correct. For JUNOS Software, licenses can be either permanent or valid until a specified date.

Displaying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the device.

Action From the CLI, enter the `show system license usage` command.

Sample Output

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

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
bgp-reflection	1	1	0	permanent

Meaning The output shows a list of the licenses installed on the device and how they are used. Verify the following information:

- Each license is present. Features are listed in ascending alphanumeric order by license name. The number of licenses is shown in the third column. Verify that the appropriate number of licenses are installed.
- The number of used licenses matches the number of configured features. If a licensed feature is configured, the feature is considered used. The sample output shows that the BGP route reflection feature is configured.
- The expiration information for the license is correct. For JUNOS Software, licenses can be either permanent or valid until a specified date.

Displaying Installed License Keys

Purpose Verify the license keys installed on the device.

Action From the CLI, enter the `show system license keys` command.

Sample Output `user@hostname> show system license keys`

```
G03000002223 aeaqea qkjjhd ambrha 3tkqkc ayareb zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbbb xdarpq
              qq53lu qcx4vm ydakcs t3yyh2 v5mq

G03000002224 aeaqea qkjjhd ambrha 3tkqkc ayargb zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbof l4uon5
              7rokz7 wgdocl r4q32p 2wu4zf zrxax

G03000002225 aeaqea qkjjhd ambrha 3tkqkc ayarab zicik6
              nv6jck btlxao 2trfyq 65cdou r5tbiu jr6ui2
              1mqgqj ouzq5a aiokdn 4tr4u2 wmcq
```

Meaning The output shows a list of the license keys installed on the device. Verify that each expected license key is present.

Chapter 20

Managing Files

You can use the J-Web interface 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 configuration editor to prevent unauthorized users from viewing sensitive configuration information.

For more information about system management, see the *JUNOS System Basics Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Before You Begin on page 323
- Managing Files with the J-Web Interface on page 323
- Cleaning Up Files with the CLI on page 328
- Managing Accounting Files on page 328
- Encrypting and Decrypting Configuration Files on page 329

Before You Begin

Before you perform any file management tasks, you must perform the initial services router configuration described in the Getting Started Guide for your device.

Managing Files with the J-Web Interface

This section contains the following topics:

- Cleaning Up Files on page 324
- Downloading Files on page 325
- Deleting Files on page 326
- Deleting the Backup Software Image on page 327

Cleaning Up Files

You can use the J-Web interface to rotate log files and delete unnecessary files on the services router. 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—All information in the current log files is archived, and fresh log files are created.
- Deletes log files in `/var/log`—Any files that are not currently being written to are deleted.
- Deletes temporary files in `/var/tmp`—Any files that have not been accessed within two days are deleted.
- Deletes all crash files in `/var/crash`—Any core files that the device has written during an error are deleted.
- Deletes all software images (*.tgz files) in `/var/sw/pkg`—Any software images copied to this directory during software upgrades are deleted.

Figure 17 on page 324 shows the Clean Up Files page.

Figure 17: Clean Up Files Page

[Manage > Files](#)

Files

Clean Up Files

If you are running low on storage space on your router, you can click on the "Clean Up Files" button below. By doing so, the router will perform the following:

- Rotate your log files
- Delete log files in `/var/log` that are not currently being written to
- Delete temporary files in `/var/tmp` that have not been touched in 2 days
- Delete all crash files in `/var/crash`

Alternatively, you can click on the "File Type" group name below to manually download and delete individual files.

[Clean Up Files](#)

Download and Delete Files

File Type	Directory	Usage
Log Files	<code>/cf/var/log</code>	9.2M
Temporary Files	<code>/cf/var/tmp</code>	48K
Crash (Core) Files	<code>/cf/var/crash</code>	1.0K

Delete Backup JUNOS Package

JUNOS normally keeps a copy of the previous software installation in case you want to revert to it. This backup can be deleted if your compact flash is becoming full. To delete the old package file, click on the link below.

Backup JUNOS Package Name	<code>/cf/packages/junos-7.5R1.1-domestic</code>
Backup JUNOS File Size	37M

[Delete backup JUNOS package](#)

To rotate log files and delete unnecessary files with the J-Web interface:

1. In the J-Web 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 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**.

Downloading Files

You can use the J-Web interface to download a copy of an individual file from the services router. When you download a file, it is not deleted from the file system.

Figure 18 on page 325 shows the J-Web page from which you can download log files.

Figure 18: Log Files Page (Download)

[Manage > Files](#)

Files

Log Files

	Name	Size	Date	Owner/Group	Action
	auditd	0B	May 29 2005	root/wheel	Download
	autod	2M	Mar 19 20:27	root/wheel	Download
	bfdd	11K	Feb 28 19:22	root/wheel	Download
	chassisd	744K	Mar 19 20:27	root/wheel	Download
	snmpd	126K	Mar 16 02:21	root/wheel	Download
	spd	48B	Mar 16 01:38	root/wheel	Download
	svj	228B	Feb 21 22:56	root/wheel	Download
	vrrpd	217K	Mar 19 20:28	root/wheel	Download

To download files with the J-Web interface:

1. In the J-Web 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 Software**—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 interface displays the files located in the directory.

3. To download an individual file, click **Download**.
4. Choose a location for the browser to save the file.

The file is downloaded.

Deleting Files

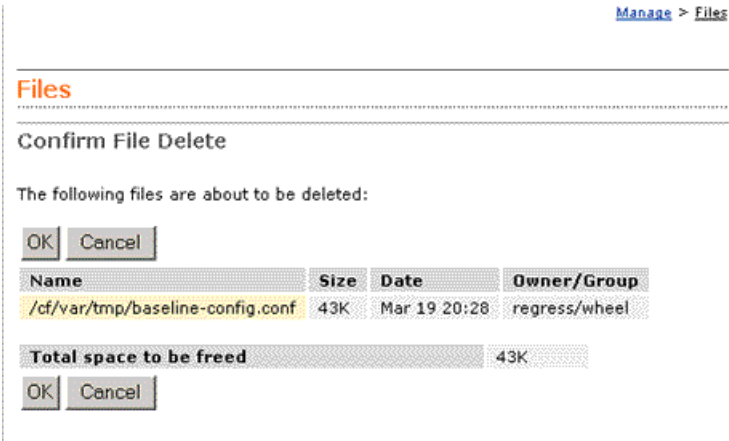
You can use the J-Web interface to delete an individual file from the services router. When you delete the file, it is permanently removed from the file system.



CAUTION: If you are unsure whether to delete a file from the device, we recommend using the **Cleanup Files** tool described in “Cleaning Up Files” on page 324. This tool determines which files can be safely deleted from the file system.

Figure 19 on page 326 shows the J-Web page on which you confirm the deletion of files.

Figure 19: Confirm File Delete Page



To delete files with the J-Web interface:

1. In the J-Web 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 Software**—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 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 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**.

Deleting the Backup Software Image

JUNOS Software 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 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 interface, select **Maintain > Files**.
2. In the Delete Backup JUNOS Package section, review the backup image information listed.
3. To delete the backup image, click the **Delete backup JUNOS package** link.
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**.

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 services router. 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—All information in the current log files is archived, old archives are deleted, and fresh log files are created.
- Deletes log files in **/var/log**—Any files that are not currently being written to are deleted.
- Deletes temporary files in **/var/tmp**—Any files that have not been accessed within two days are deleted.
- Deletes all crash files in **/var/crash**—Any core files that the device has written during an error are deleted.
- Deletes all software images (*.tgz files) in **/var/sw/pkg**—Any software images copied to this directory during software upgrades are deleted.

To rotate log files and delete unnecessary files with the CLI:

1. Enter operational mode in the CLI.
2. To rotate log files and identify the files that can be safely deleted, enter the following command:

```
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.

Managing Accounting Files

If you configure your system to capture accounting data in log files, set the location for accounting files to the DRAM.

The default location for accounting files is the **cfs/var/log** directory on the CompactFlash card. The **nonpersistent** option minimizes the read/write traffic to your CompactFlash 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 CompactFlash card:

1. Enter the configuration mode in the CLI.
2. To create an accounting data log file in DRAM, enter the following command, replacing *filename* with the name of the file:

```
user@host> edit accounting-options file filename
```

3. To store accounting log files in the DRAM file, enter the following command:

```
user@host> set file filename nonpersistent
```

For more information about the `nonpersistent` option, see the *JUNOS Network Management Configuration Guide*.



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.

Encrypting and Decrypting Configuration Files

Configuration files contain sensitive information such as IP addresses. By default, the device stores configuration files in unencrypted format on an external CompactFlash card. This storage method is considered a security risk because the CompactFlash card can easily be removed from the device. To prevent unauthorized users from viewing sensitive information in configuration files, you can encrypt them.

If your device runs the Canada and U.S. version of JUNOS Software, the configuration files can be encrypted with the Advanced Encryption Standard (AES) or Data Encryption Standard (DES) encryption algorithms. If your device runs the international version of JUNOS Software, the files can be encrypted only with DES.

To prevent unauthorized access, the encryption key is stored in the device's EEPROM. You can copy the encrypted configuration files to another device and decrypt them if that device has the same encryption key. To prevent encrypted configuration files from being copied to another device and decrypted, you can set a unique encryption key that contains the chassis serial number of your device. Configuration files that are encrypted with a unique encryption key cannot be decrypted on any other device.

The encryption process encrypts only the configuration files in the `/config` and `/var/db/config` directories. Files in subdirectories under these directories are not encrypted. The filenames of encrypted configuration files have the extension `.gz.jc`—for example, `juniper.conf.gz.jc`.



NOTE: You must have superuser privileges to encrypt or decrypt configuration files.

This section contains the following topics:

- Encrypting Configuration Files on page 330
- Decrypting Configuration Files on page 331
- Modifying the Encryption Key on page 331

Encrypting Configuration Files

To encrypt configuration files on a device:

1. Enter operational mode in the CLI.
2. To configure an encryption key in EEPROM and determine the encryption process, enter one of the **request system set-encryption-key** commands described in Table 191 on page 330.

Table 191: request system set-encryption-key Commands

CLI Command	Description
<code>request system set-encryption-key</code>	Sets the encryption key and enables default configuration file encryption as follows: <ul style="list-style-type: none"> ■ AES encryption for the Canada and U.S. version of JUNOS Software ■ DES encryption for the international version of JUNOS Software
<code>request system set-encryption-key algorithm des</code>	Sets the encryption key and specifies configuration file encryption by DES.
<code>request system set-encryption-key unique</code>	Sets the encryption key and enables default configuration file encryption with a unique encryption key that includes the chassis serial number of the device. 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.
<code>request system set-encryption-key des unique</code>	Sets the encryption key and specifies configuration file encryption by DES with a unique encryption key.

For example:

```
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 6 characters.

```
Enter EEPROM stored encryption key:juniper1
```

```
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the encryption key.
5. Enter configuration mode in the CLI.

6. To enable configuration file encryption to take place, enter the following commands:

```
user@host# edit system
```

```
user@host# set encrypt-configuration-files
```

7. To begin the encryption process, commit the configuration.

```
user@host# commit
```

```
commit complete
```

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. To verify your permission to decrypt configuration files on this device, enter the following command and 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. To enable configuration file decryption, enter the following commands:

```
user@host# edit system
```

```
user@host# set no-encrypt-configuration-files
```

6. To begin the decryption process, commit the configuration.

```
user@host# commit
```

```
commit complete
```

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. To configure a new encryption key in EEPROM and determine the encryption process, enter one of the **request system set-encryption-key** commands described in Table 191 on page 330. For example:

```
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 6 characters.

```
Enter EEPROM stored encryption key:juniperone
```

```
Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the new encryption key.

Part 5

Diagnosing Performance and Network Problems

- Using Diagnostic Tools on page 335
- Configuring Packet Capture on page 381
- Configuring RPM Probes on page 395

Chapter 21

Using Diagnostic Tools

J Series Services Routers and SRX Series Services Gateways 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.

For complete descriptions of CLI operational mode commands, see the *JUNOS System Basics and Services Command Reference*, the *JUNOS Interfaces Command Reference*, and the *JUNOS Routing Protocols and Policies Command Reference*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Diagnostic Terms on page 335
- Diagnostic Tools Overview on page 336
- Before You Begin on page 341
- Pinging Hosts from the J-Web Interface on page 341
- Checking MPLS Connections from the J-Web Interface on page 345
- Tracing Unicast Routes from the J-Web Interface on page 350
- Capturing and Viewing Packets with the J-Web Interface on page 354
- Using CLI Diagnostic Commands on page 359

Diagnostic Terms

Before diagnosing your device, become familiar with the terms defined in Table 192 on page 335.

Table 192: Diagnostic Terms

Term	Definition
Don't Fragment (DF) bit	Bit in the IP header that instructs routers not to fragment a packet. You might set this bit if the destination host cannot reassemble the packet or if you want to test the path maximum transmission unit (MTU) for a destination host.

Table 192: Diagnostic Terms (*continued*)

Term	Definition
routing instance	Collection of routing tables, interfaces, and routing protocol interfaces. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables.
loose source routing	Option in the IP header used to route a packet based on information supplied by the source. A gateway or host must route the packet using the routers specified by this information, but the packet can use other routers along the way.
strict source routing	Option in the IP header used to route a packet based on information supplied by the source. A gateway or host must route the packet exactly as specified by this information.
time to live (TTL)	Value (octet) in the IP header that is (usually) decremented by 1 for each hop the packet passes through. If the field reaches zero, the packet is discarded and a corresponding error message is sent to the source of the packet.
type of service (TOS)	Value (octet) in the IP header that defines the service the source host requests, such as the packet's priority and the preferred delay, throughput, and reliability.

Diagnostic Tools Overview

Use the J-Web Diagnose options to diagnose a device. J-Web results are displayed in the browser.

You can also diagnose 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.

This section contains the following topics. To filter output to a file, see “Filtering Command Output” on page 148.

- J-Web Diagnostic Tools Overview on page 336
- CLI Diagnostic Commands Overview on page 337
- MPLS Connection Checking on page 339

J-Web Diagnostic Tools Overview

The J-Web diagnostic tools consist of the options that appear when you select **Troubleshoot** and **Maintain** in the task bar. Table 193 on page 336 describes the functions of the Diagnose and Manage options.

Table 193: J-Web Interface Diagnose and Manage Options

Option	Function
Troubleshoot Options	
Ping Host	Allows you to ping a remote host. You can configure advanced options for the ping operation. For details, see “Using the J-Web Ping Host Tool” on page 342.

Table 193: J-Web Interface Diagnose and Manage Options (continued)

Option	Function
Ping MPLS	Allows you to ping an MPLS endpoint using various options. For details, see “MPLS Connection Checking” on page 339.
Traceroute	Allows you to trace a route between the device and a remote host. You can configure advanced options for the traceroute operation. For details, see “Tracing Unicast Routes from the J-Web Interface” on page 350.
Packet Capture	Allows you to capture and analyze router control traffic. For details, see “Capturing and Viewing Packets with the J-Web Interface” on page 354.
Maintain Options	
Files	Allows you manage log, temporary, and core files on the device. For details, see “Managing Files with the J-Web Interface” on page 323.
Upgrade	Allows you to upgrade and manage device software packages. For details, see “Performing Software Upgrades and Reboots” on page 251.
Licenses	Displays a summary of the licenses needed and used for each feature that requires a license. Allows you to add licenses. For details, see the <i>JUNOS Software Administration Guide</i> .
Reboot	Allows you to reboot the device at a specified time. For details, see “Rebooting or Halting the Device with the J-Web Interface” on page 269.

CLI Diagnostic Commands Overview

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 interface. Instead of invoking the tools through a graphical interface, you use operational mode commands to perform the tasks.

Because the CLI is a superset of the J-Web interface, 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 194 on page 338.

Table 194: CLI Diagnostic Command Summary

Command	Function
Controlling the CLI Environment	
set <i>option</i>	Configures the CLI display.
Diagnosis and Troubleshooting	
clear	Clears statistics and protocol database information.
mtrace	Traces information about multicast paths from source to receiver. For details, see “Tracing Multicast Routes from the CLI” on page 369.
monitor	Performs real-time debugging of various software components, including the routing protocols and interfaces. For details, see the following sections: <ul style="list-style-type: none"> ■ Using the monitor interface Command on page 373 ■ Using the monitor traffic Command on page 375 ■ Displaying Log and Trace Files from the CLI on page 373
ping	Determines the reachability of a remote network host. For details, see “Pinging Hosts from the CLI” on page 359.
ping mpls	Determines the reachability of an MPLS endpoint using various options. For details, see “MPLS Connection Checking” on page 339.
test	Tests the configuration and application of policy filters and AS path regular expressions.
traceroute	Traces the route to a remote network host. For details, see “Tracing Unicast Routes from the CLI” on page 365.
Connecting to Other Network Systems	
ssh	Opens secure shell connections. For details, see “Using the ssh Command” on page 63.
telnet	Opens Telnet sessions to other hosts on the network. For details, see “Using the telnet Command” on page 62.
Management	
copy	Copies files from one location on the device to another, from the device to a remote system, or from a remote system to the device.
restart <i>option</i>	Restarts the various system processes, including the routing protocol, interface, and SNMP processes.
request	Performs system-level operations, including stopping and rebooting the device and loading software images.

Table 194: CLI Diagnostic Command Summary (*continued*)

Command	Function
start	Exits the CLI and starts a UNIX shell.
configuration	Enters configuration mode. For details, see the <i>JUNOS Software Administration Guide</i> .
quit	Exits the CLI and returns to the UNIX shell.

MPLS Connection Checking

Use either the J-Web ping MPLS diagnostic tool or the CLI `ping mpls` command 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 195 on page 339 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 195: Options for Checking MPLS Connections

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping RSVP-signaled LSP	ping mpls rsvp	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The 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.

Table 195: Options for Checking MPLS Connections (*continued*)

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping LDP-signaled LSP	ping mpls ldp	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The 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.
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) router'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 router 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.	For information about interface names, See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i> .
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.	

Before You Begin

This section includes the following topics:

- General Preparation on page 341
- Ping MPLS Preparation on page 341

General Preparation

To use the J-Web interface and CLI operational tools, you must have the appropriate access privileges. For more information about configuring access privilege levels, see “Adding New Users” on page 51 and the *JUNOS System Basics Configuration Guide*.

Ping MPLS Preparation

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.”

Pinging Hosts from the J-Web Interface

This section contains the following topics:

- Using the J-Web Ping Host Tool on page 342
- Ping Host Results and Output Summary on page 344

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 “Pinging Hosts from the CLI” on page 359.)

To use the ping host tool:

1. Select **Troubleshoot > Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 20 on page 343).
3. Enter information into the Ping Host page, as described in Table 196 on page 343.

The Remote Host field is the only required field.

4. Click **Start**.

The results of the ping operation are displayed in the main pane (see Figure 21 on page 344). 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
```

Table 197 on page 345 summarizes the output fields of the display.

5. To stop the ping operation before it is complete, click **OK**.

Figure 20: Ping Host Page

[Diagnose](#) > [Ping Host](#)

Ping Host

Ping Host

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

Entering a host below creates a periodic ping task that will run until cancelled or until it times out as specified.

* Remote Host

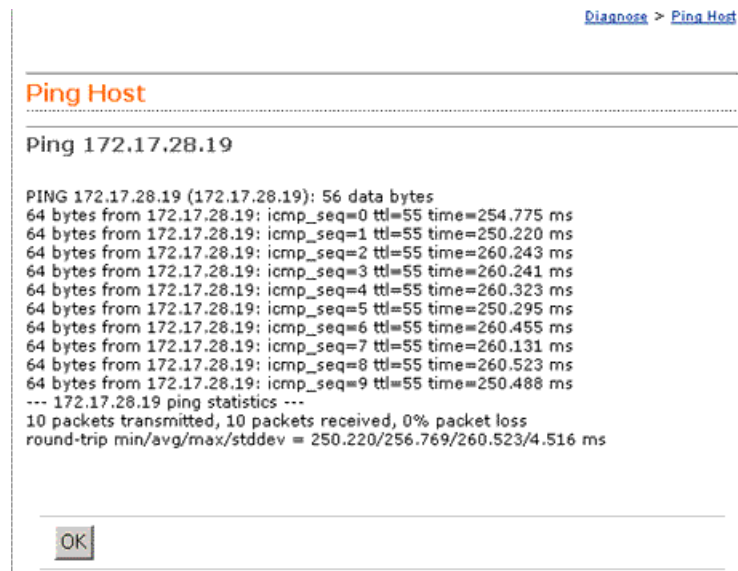
Advanced options

Table 196: J-Web Ping Host Field Summary

Field	Function	Your Action
Remote Host	Identifies the host to ping.	Type the hostname or IP address of the host to ping.
Advanced Options		
Don't Resolve Addresses	Determines whether to display hostnames of the hops along the path.	<ul style="list-style-type: none"> ■ To suppress the display of the hop hostnames, select the check box. ■ To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the interface on which ping requests are sent. If you select any , the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send.
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"> ■ To set the DF bit, select the check box. ■ To clear the DF bit, clear the check box.
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"> ■ To record and display the path of the packet, select the check box. ■ To suppress the recording and display of the path of the packet, clear the check box.
Type-of-Service	Specifies the type-of-service (TOS) value in the IP header of the ping request packet.	From the list, select the decimal value of the TOS field.
Routing Instance	Name of the routing instance for the ping attempt.	From the list, select the routing instance name.

Table 196: J-Web Ping Host Field Summary (continued)

Field	Function	Your Action
Interval	Specifies the interval, in seconds, between the transmission of each ping request.	From the list, select the interval.
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 65468. 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.	From the list, select the TTL.
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"> ■ To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box. ■ To route the ping requests using the routing table, clear the check box.

Figure 21: Ping Host Results Page

Ping Host Results and Output Summary

Table 197 on page 345 summarizes the output in the ping host display. If the device receives no ping responses from the destination host, review the list after Table 197 on page 345 for a possible explanation.

Table 197: J-Web Ping Host Results and Output Summary

Ping Host Result	Description
<i>bytes bytes from ip-address</i>	<ul style="list-style-type: none"> ■ <i>bytes</i>—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8. ■ <i>ip-address</i>—IP address of destination host that sent the ping response packet.
<i>icmp_seq=0</i> <i>icmp_seq=number</i>	<i>number</i> —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>	<i>number</i> —Time-to-live hop-count value of the ping response packet.
<i>time=time</i>	<i>time</i> —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.
<i>number packets transmitted</i>	<i>number</i> —Number of ping requests (probes) sent to host.
<i>number packets received</i>	<i>number</i> —Number of ping responses received from host.
<i>percentage packet loss</i>	<i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage.
<i>round-trip min/avg/max/stddev = min-time/avg-time/max-time/std-dev ms</i>	<ul style="list-style-type: none"> ■ <i>min-time</i>—Minimum round-trip time (see <i>time=time</i> field in this table). ■ <i>avg-time</i>—Average round-trip time. ■ <i>max-time</i>—Maximum round-trip time. ■ <i>std-dev</i>—Standard deviation of the round-trip times.

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.

For more information about ICMP, see RFC 792, *Internet Control Message Protocol*.

Checking MPLS Connections from the J-Web Interface

Use the J-Web ping MPLS diagnostic tool to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 VPNs, and Layer 2 circuits.

Alternatively, you can use the CLI commands `ping mpls`, `ping mpls l2circuit`, `ping mpls l2vpn`, and `ping mpls l3vpn`. For more information, see “Pinging Hosts from the CLI” on page 359.

Before using the J-Web ping MPLS tool in your network, read “Ping MPLS Preparation” on page 341.

This section contains the following topics:

- Using the J-Web Ping MPLS Tool on page 346
- Ping MPLS Results and Output on page 349

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 (see Figure 22 on page 347).
3. Enter information into the Ping MPLS page, as described in Table 198 on page 347.
4. Click **Start**.

Table 199 on page 350 summarizes the output fields of the display.

5. To stop the ping operation before it is complete, click **OK**.

Figure 22: Ping MPLS Page

[Diagnose](#) > [Ping MPLS](#)

Ping MPLS

Ping MPLS

Use the Ping MPLS diagnostic tool to send variations of ICMP "echo request" packets to the specified MPLS endpoint.

☐ Ping RSVP-signaled LSP

* LSP Name ?
 Count ?

Source Address ?
 Detailed Output ☐ ?

☐ Ping LDP-signaled LSP

☐ Ping LSP to Layer 3 VPN prefix

☐ Ping LSP for a Layer 2 VPN connection by interface

☐ Ping LSP for a Layer 2 VPN connection by instance

☐ Ping LSP to a Layer 2 circuit remote site by interface

☐ Ping LSP to a Layer 2 circuit remote site by VCI

☐ Ping end point of LSP

Table 198: J-Web Ping MPLS Field Summary

Field	Function	Your Action
Ping RSVP-signaled LSP		
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.	From the list, select the number of ping requests to send. 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.
Ping LDP-signaled LSP		
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.	From the list, select the number of ping requests to send. 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 198: J-Web Ping MPLS Field Summary (continued)

Field	Function	Your Action
Ping LSP to Layer 3 VPN prefix		
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.	From the list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
VPN Prefix	Identifies the IP address prefix and length of the Layer 3 VPN to ping.	Type the IP address prefix and length of the VPN to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a J Series device interface.
Locate LSP using interface name		
Interface	Specifies the interface on which the ping requests are sent. (See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i> .)	From the list, select the J Series device interface on which ping requests are sent. If you select any , 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.	From the list, select the number of ping requests to send. 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.
Instance to which this connection belongs		
Layer 2 VPN 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.	From the list, select the number of ping requests to send. 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.
Locate LSP from interface name		

Table 198: J-Web Ping MPLS Field Summary (continued)

Field	Function	Your Action
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the J Series device interface on which ping requests are sent. If you select any , 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.	From the list, select the number of ping requests to send. 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.
Locate LSP from virtual circuit information		
Remote Neighbor	Identifies the remote neighbor (PE router) 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.	From the list, select the number of ping requests to send.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping end point of LSP		
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.	From the list, select the number of ping requests to send.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.

Ping MPLS Results and Output

Table 199 on page 350 summarizes the output in the ping MPLS display. If the device receives no responses from the destination host, review the list after Table 199 on page 350 for a possible explanation.

Table 199: 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.

Tracing Unicast Routes from the J-Web Interface

You can use the traceroute diagnostic tool to display a list of routers 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 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.

Alternatively, you can use the CLI **traceroute** command to generate the list.

This section contains the following topics:

- Using the J-Web Traceroute Tool on page 351
- Traceroute Results and Output Summary on page 353

Using the J-Web Traceroute Tool

To use the traceroute tool:

1. Select **Troubleshoot > Traceroute**.
2. Next to Advanced options, click the expand icon (see Figure 23 on page 352).
3. Enter information into the Traceroute page, as described in Table 200 on page 352.

The **Remote Host** field is the only required field.

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 displays the round-trip time for each traceroute operation. If the device times out before receiving a **Time Exceeded** message, an asterisk (*) is displayed for that round-trip time.

Table 201 on page 353 summarizes the output fields of the display.

5. To stop the traceroute operation before it is complete, click **OK** while the results of the traceroute operation are being displayed.

Figure 23: Traceroute Page

[Diagnose](#) > [Traceroute](#)

Traceroute

Traceroute to Host

The traceroute diagnostic tool uses a series of packets crafted to elicit an ICMP "time exceeded" messages from intermediate points in the network between your router and the specified host.

The time-to-live for a packet is decremented each time the packet is routed, so traceroute generally receives at least one "time exceeded" response from each waypoint. Traceroute starts with a packet with a time-to-live value of one, and increments the time to live for subsequent packets, thereby constructing a rudimentary map of the path between hosts.

Entering a host below creates a traceroute task that will run until the traceroute is complete or until it fails due to time out.

• Remote Host ?

+ Advanced options

Table 200: Traceroute Field Summary

Field	Function	Your Action
Remote Host	Identifies the destination host of the traceroute.	Type the hostname or IP address of the destination host.
Advanced Options		
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"> ■ To suppress the display of the hop hostnames, select the check box. ■ To display the hop hostnames, clear the check box.
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"> ■ To bypass the routing table and send the traceroute packets to hosts on the specified interface only, select the check box. ■ To route the traceroute packets by means of the routing table, clear the check box.
Interface	Specifies the interface on which the traceroute packets are sent.	From the list, select the interface on which traceroute packets are sent. If you select any , 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.	From the list, select the TTL.

Table 200: Traceroute Field Summary (*continued*)

Field	Function	Your Action
Type-of-Service	Specifies the type-of-service (TOS) value to include in the IP header of the traceroute request packet.	From the list, select the decimal value of the TOS field.
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"> ■ To display the AS numbers, select the check box. ■ To suppress the display of the AS numbers, clear the check box.

Traceroute Results and Output Summary

Table 201 on page 353 summarizes the output in the traceroute display. If the device receives no responses from the destination host, review the list after Table 201 on page 353 for a possible explanation.

Table 201: J-Web Traceroute Results and Output Summary

Field	Description
<i>hop-number</i>	Number of the hop (router) along the path.
<i>host</i>	Hostname, if available, or IP address of the router. If the Don't Resolve Addresses check box is selected, the hostname is not displayed.
<i>ip-address</i>	IP address of the router.
<i>as-number</i>	AS number of the router.
<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 router.
<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 router.
<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 router.

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 router 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.

For more information about ICMP, see RFC 792, *Internet Control Message Protocol*.

Capturing and Viewing Packets with the J-Web Interface

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 interface allows you to capture traffic destined for or originating from the Routing Engine. You can use J-Web packet capture 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 using packet analyzers such as Ethereal. J-Web packet capture does not capture transient traffic.

Alternatively you can use the CLI **monitor traffic** command to capture and display packets matching a specific criteria. For details, see “Using the monitor traffic Command” on page 375.

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 “Configuring Packet Capture” on page 381.

This section contains the following topics:

- Using J-Web Packet Capture on page 354
- Packet Capture Results and Output Summary on page 357

Using J-Web Packet Capture

To use J-Web packet capture:

1. Select **Troubleshoot > Packet Capture**.
2. Enter information into the Packet Capture page (Figure 24 on page 355) as described in Table 202 on page 355.

The sample configuration in Table 202 on page 355 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. To save the captured packets to a file, or specify other advanced options, click the expand icon next to Advanced options, and enter information as described in Table 202 on page 355.
4. Click **Start**.

The captured packet headers are decoded and displayed in the Packet Capture display (see Figure 25 on page 358).

Table 203 on page 358 summarizes the output fields of the 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**.

Figure 24: Packet Capture Page

Table 202: Packet Capture Field Summary

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured. If you select default , packets on the Ethernet management port 0, are captured.	From the list, select an interface—for example, ge-0/0/0.
Detail level	Specifies the extent of details to be displayed for the packet headers. <ul style="list-style-type: none"> ■ Brief—Displays the minimum packet header information. This is the default. ■ Detail—Displays packet header information in moderate detail. ■ Extensive—Displays the maximum packet header information. 	From the list, select Detail .

Table 202: Packet Capture Field Summary (*continued*)

Field	Function	Your Action
Packets	Specifies the number of packets to be captured. Values range from 1 to 1000. Default is 10. Packet capture stops capturing packets after this number is reached.	From the list, select the number of packets to be captured—for example, 10 .
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"> ■ Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both. ■ Type—Specifies if packet headers are matched for host address or network address. <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"> 1. From the Direction list, select source. 2. From the Type list, select host. 3. In the Address box, type 10.1.40.48. 4. Click Add.
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.	From the list, select a protocol—for example, tcp .
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"> 1. From the Type list, select src. 2. In the Port box, type 23.
Advanced Options		
Absolute TCP Sequence	Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.	<ul style="list-style-type: none"> ■ To display absolute TCP sequence numbers in the packet headers, select this check box. ■ To stop displaying absolute TCP sequence numbers in the packet headers, clear this check box.
Layer 2 Headers	Specifies that link-layer packet headers are to be displayed.	<ul style="list-style-type: none"> ■ To include link-layer packet headers while capturing packets, select this check box. ■ To exclude link-layer packet headers while capturing packets, clear this check box.
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"> ■ To read all packets that reach the interface, select this check box. ■ To read only packets addressed to the interface, clear this check box.
Display Hex	Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.	<ul style="list-style-type: none"> ■ To display the packet headers in hexadecimal format, select this check box. ■ To stop displaying the packet headers in hexadecimal format, clear this check box.

Table 202: Packet Capture Field Summary (*continued*)

Field	Function	Your Action
Display ASCII and Hex	Specifies that packet headers are to be displayed in hexadecimal and ASCII format.	<ul style="list-style-type: none"> ■ To display the packet headers in ASCII and hexadecimal formats, select this check box. ■ To stop displaying the packet headers in ASCII and hexadecimal formats, clear this check box.
Header Expression	<p>Specifies the match condition for the packets to be captured.</p> <p>The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.</p>	You can enter match conditions directly in this field 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, 256 .
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"> ■ To prevent packet capture from resolving IP addresses to hostnames, select this check box. ■ To resolve IP addresses into hostnames, clear this check box.
No Timestamp	Suppresses the display of packet header timestamps.	<ul style="list-style-type: none"> ■ To stop displaying timestamps in the captured packet headers, select this check box. ■ To display the timestamp in the captured packet headers, clear this check box.
Write Packet Capture File	<p>Writes the captured packets to a file in PCAP format in <code>/var/tmp</code>. The files are named with the prefix <code>jweb-pcap</code> and the extension <code>.pcap</code>.</p> <p>If you select this option, the decoded packet headers are not displayed on the packet capture page.</p>	<ul style="list-style-type: none"> ■ To save the captured packet headers to a file, select this check box. ■ To decode and display the packet headers on the J-Web page, clear this check box.

Packet Capture Results and Output Summary

Figure 25 on page 358 shows J-Web packet capture output from **router1**, with the level of detail set to **brief**. Table 203 on page 358 summarizes the output in the packet capture display.

Figure 25: Packet Capture Results Page

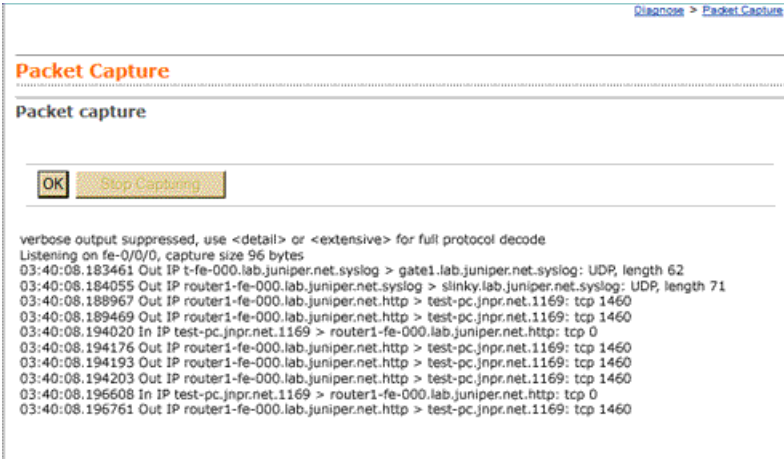


Table 203: J-Web Packet Capture Results and Output Summary

Field	Description
<i>timestamp</i>	Time when the packet was captured. The timestamp 00:45:40.823971 means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds. NOTE: The time displayed is local time.
<i>direction</i>	Direction of the packet. Specifies whether the packet originated from the Routing Engine (Out), or was destined for the Routing Engine (In).
<i>protocol</i>	Protocol for the packet. In the sample output, IP 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 is displayed. NOTE: 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 are displayed. NOTE: 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, TCP indicates the Layer 4 protocol.
<i>data size</i>	Size of the packet (in bytes).

Using CLI Diagnostic Commands

Because the CLI is a superset of the J-Web interface, you can perform certain tasks only through the CLI. For an overview of the CLI operational mode commands, along with instructions for filtering command output, see “CLI Diagnostic Commands Overview” on page 337.

This section contains the following topics:

- Pinging Hosts from the CLI on page 359
- Checking MPLS Connections from the CLI on page 361
- Tracing Unicast Routes from the CLI on page 365
- Tracing Multicast Routes from the CLI on page 369
- Displaying Log and Trace Files from the CLI on page 373
- Monitoring Interfaces and Traffic from the CLI on page 373

Pinging Hosts from 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.

Alternatively, you can use the J-Web interface. (See “Using the J-Web Ping Host Tool” on page 342.)

Enter the **ping** command with the following syntax. Table 204 on page 359 describes the **ping** command options.

```
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>
```

To quit the **ping** command, press Ctrl-C.

Table 204: 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.

Table 204: CLI ping Command Options (*continued*)

Option	Description
bypass-routing	(Optional) Bypasses the routing tables and sends the ping requests only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. Use this option to ping a local system through an interface that has no route through it.
countnumber	(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.
do-not-fragment	(Optional) Sets the Don't Fragment (DF) bit in the IP header of the ping request packet.
inet	(Optional) Forces the ping requests to an IPv4 destination.
inet6	(Optional) Forces the ping requests to an IPv6 destination.
interval seconds	(Optional) Sets the interval between ping requests, in seconds. Specify an interval from 0.1 through 10,000. The default value is 1 second.
loose-source [hosts]	(Optional) For IPv4, sets the loose source routing option in the IP header of the ping request packet.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
pattern string	(Optional) Includes the hexadecimal string you specify, in the ping request packet.
rapid	(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 count option.
record-route	(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.
routing-instance routing-instance-name	(Optional) Uses the routing instance you specify for the ping request.
size bytes	(Optional) Sets the size of the ping request packet. Specify a size from 0 through 65,468. The default value is 56 bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.
source source-address	(Optional) Uses the source address that you specify, in the ping request packet.
strict	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.
strict-source [hosts]	(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.
tos number	(Optional) Sets the type-of-service (TOS) value in the IP header of the ping request packet. Specify a value from 0 through 255.
ttl number	(Optional) Sets the time-to-live (TTL) value for the ping request packet. Specify a value from 0 through 255.

Table 204: CLI ping Command Options (continued)

Option	Description
wait seconds	(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 10 seconds. If you use this option without the count option, the J Series device uses a default count of 5 packets.
detail	(Optional) Displays the interface on which the ping response was received.
verbose	(Optional) Displays detailed output.

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. For information, see “Ping Host Results and Output Summary” on page 344.

Checking MPLS Connections from the CLI

Use the **ping mpls** commands to diagnose the state of LSPs, Layer 2 and Layer 3 VPNs, and Layer 2 circuits. When you issue a command from a J Series device operating as the inbound 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 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.

Alternatively, you can use the J-Web ping MPLS tool. For more information, see “Checking MPLS Connections from the J-Web Interface” on page 345.

Before using **ping mpls** commands in your network, read “Ping MPLS Preparation” on page 341.

The **ping mpls** commands diagnose the connectivity of MPLS and VPN networks in the following ways:

- Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs on page 362
- Pinging Layer 3 VPNs on page 363

- Pinging Layer 2 VPNs on page 363
- Pinging Layer 2 Circuits on page 365

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs

Enter the `ping mpls` command with the following syntax. Table 205 on page 362 describes the `ping mpls` command options.

```
user@host> ping mpls (ldp fec | lsp-end-point prefix-name | rsvp lsp-name)
<exp forwarding-class> <count number> <source source-address> <detail>
```

To quit the `ping mpls` command, press Ctrl-C.

Alternatively, you can use the J-Web interface. (See “Checking MPLS Connections from the J-Web Interface” on page 345.)

Table 205: CLI `ping mpls ldp` and `ping mpls lsp-end-point` Command Options

Option	Description
<code>ldp fec</code>	Pings an LDP-signaled LSP identified by the forwarding equivalence class (FEC) prefix and length.
<code>lsp-end-point prefix-name</code>	Pings an LSP endpoint using either an LDP FEC or a RSVP LSP endpoint address.
<code>rsvp lsp-name</code>	Pings an RSVP-signaled LSP identified by the specified LSP name.
<code>exp forwarding-class</code>	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
<code>count number</code>	(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.
<code>source source-address</code>	(Optional) Uses the source address that you specify, in the ping request packet.
<code>detail</code>	(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.

Following is sample output from a `ping mpls` command:

```
user@host> ping mpls rsvp count 5
!!xxx
--- lsping statistics ---
5 packets transmitted, 2 packets received, 60% packet loss
3 packets received with error status, not counted as received.
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool. For information, see “Ping MPLS Results and Output” on page 349.

Pinging Layer 3 VPNs

Enter the `ping mpls l3vpn` command with the following syntax. Table 206 on page 363 describes the `ping mpls l3vpn` command options.

```
user@host> ping mpls l3vpn prefix prefix-name <l3vpn-name> <bottom-label-ttl>
<exp forwarding-class> <count number> <source source-address> <detail>
```

To quit the `ping mpls l3vpn` command, press Ctrl-C.

Alternatively, you can use the J-Web interface. (See “Checking MPLS Connections from the J-Web Interface” on page 345.)

Table 206: CLI ping mpls l3vpn Command Options

Option	Description
<code>l3vpn prefix <i>prefix-name</i></code>	Pings the remote host specified by the prefix to verify that the prefix is present in the PE router's VPN routing and forwarding (VRF) table. This option does not test the connectivity between a PE router and a CE router.
<code><i>l3vpn-name</i></code>	(Optional) Layer 3 VPN name.
<code>bottom-label-ttl</code>	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
<code>exp <i>forwarding-class</i></code>	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
<code>count<i>number</i></code>	(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.
<code>source <i>source-address</i></code>	(Optional) Uses the source address that you specify, in the ping request packet.
<code>detail</code>	(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.

Following is sample output from a `ping mpls l3vpn` command:

```
user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32
!!!!!!
--- l3ping 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. For information, see “Ping MPLS Results and Output” on page 349.

Pinging Layer 2 VPNs

Enter the `ping mpls l2vpn` command with the following syntax. Table 207 on page 364 describes the `ping mpls l2vpn` command options.

```

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>

```

To quit the ping mpls l2vpn command, press Ctrl-C.

Alternatively, you can use the J-Web interface. (See “Checking MPLS Connections from the J-Web Interface” on page 345.)

Table 207: CLI ping mpls l2vpn Command Options

Option	Description
<i>l2vpn interface interface-name</i>	Sends ping requests out the specified interface configured for the Layer 2 VPN on the outbound (egress) PE router.
<i>l2vpn instance l2vpn-instance-name local-site-id local-site-id-number remote-site-id 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 routers.
<i>bottom-label-ttl</i>	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
<i>exp forwarding-class</i>	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
<i>count number</i>	(Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
<i>source source-address</i>	(Optional) Uses the source address that you specify, in the ping request packet.
<i>detail</i>	(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.

Following is sample output from a ping mpls l2vpn command:

```

user@host> ping mpls l2vpn instance vpn1 remote-site-id 1 local-site-id 2 detail
Request for seq 1, to interface 68, labels <800001, 100176>
Reply for seq 1, return code: Egress-ok
Request for seq 2, to interface 68, labels <800001, 100176>
Reply for seq 2, return code: Egress-ok
Request for seq 3, to interface 68, labels <800001, 100176>
Reply for seq 3, return code: Egress-ok
Request for seq 4, to interface 68, labels <800001, 100176>
Reply for seq 4, return code: Egress-ok
Request for seq 5, to interface 68, labels <800001, 100176>
Reply for seq 5, return code: Egress-ok

--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss

```


The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool. For information, see “Ping MPLS Results and Output” on page 349.

Pinging Layer 2 Circuits

Enter the `ping mpls l2circuit` command with the following syntax. Table 208 on page 365 describes the `ping mpls l2circuit` command options.

```
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>
```

To quit the `ping mpls l2circuit` command, press Ctrl-C.

Alternatively, you can use the J-Web interface. (See “Checking MPLS Connections from the J-Web Interface” on page 345.)

Table 208: CLI ping mpls l2circuit Command Options

Option	Description
<code>l2circuit interface interface-name</code>	Sends ping requests out the specified interface configured for the Layer 2 circuit on the outbound PE router.
<code>l2circuit virtual-circuit neighbor prefix-name virtual-circuit-id</code>	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.
<code>exp forwarding-class</code>	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
<code>countnumber</code>	(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.
<code>source source-address</code>	(Optional) Uses the source address that you specify, in the ping request packet.
<code>detail</code>	(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.

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. For information, see “Ping MPLS Results and Output” on page 349.

Tracing Unicast Routes from the CLI

Use the CLI `traceroute` command to display a list of routers between the device and a specified destination host. This command 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 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.

Alternatively, you can use the J-Web interface. (See “Tracing Unicast Routes from the J-Web Interface” on page 350.)

The **traceroute monitor** command combines ping and traceroute functionality to display real-time monitoring information about each router between the J Series device and a specified destination host.

This section contains the following topics. For more information about **traceroute** commands, see the *JUNOS System Basics and Services Command Reference*.

- Using the traceroute Command on page 366
- Using the traceroute monitor Command on page 367

Using the traceroute Command

To display a list of routers between the device and a specified destination host, enter the **traceroute** command with the following syntax. Table 209 on page 366 describes the **traceroute** command options.

```
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>
<ttl number> <wait seconds>
```

To quit the **traceroute** command, press Ctrl-C.

Table 209: 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>	<p>(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.</p> <p>Use this option to display a route to a local system through an interface that has no route through it.</p>
<i>gateway address</i>	(Optional) Uses the gateway you specify to route through.

Table 209: CLI traceroute Command Options (*continued*)

Option	Description
<code>inet</code>	(Optional) Forces the traceroute packets to an IPv4 destination.
<code>inet6</code>	(Optional) Forces the traceroute packets to an IPv6 destination.
<code>no-resolve</code>	(Optional) Suppresses the display of the hostnames of the hops along the path.
<code>routing-instance</code> <code>routing-instance-name</code>	(Optional) Uses the routing instance you specify for the traceroute.
<code>source address</code>	(Optional) Uses the source address that you specify, in the traceroute packet.
<code>tos number</code>	(Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255.
<code>ttl number</code>	(Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 128.
<code>wait seconds</code>	(Optional) Sets the maximum time to wait for a response.

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. For information, see “Traceroute Results and Output Summary” on page 353.

Using the traceroute monitor Command

To display real-time monitoring information about each router between the J Series device and a specified destination host, enter the `traceroute monitor` command with the following syntax. Table 210 on page 367 describes the `traceroute monitor` command options.

```
user@host> traceroute monitor host <count number> <inet | inet6> <interval seconds>
<no-resolve> <size bytes><source source-address> <summary>
```

To quit the `traceroute monitor` command, press `Q`.

Table 210: CLI traceroute monitor Command Options

Option	Description
<code>host</code>	Sends traceroute packets to the hostname or IP address you specify.

Table 210: CLI traceroute monitor Command Options (*continued*)

Option	Description
count <i>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.
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.
interval <i>seconds</i>	(Optional) Sets the interval between ping requests, in seconds. The default value is 1 second.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
size <i>bytes</i>	(Optional) Sets the size of the ping request packet. The size can be from 0 through 65468 bytes. The default packet size is 64 bytes.
source <i>address</i>	(Optional) Uses the source address that you specify, in the traceroute packet.
summary	(Optional) Displays the summary traceroute information.

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 211 on page 368 summarizes the output fields of the display.

Table 211: CLI traceroute monitor Command Output Summary

Field	Description
host	Hostname or IP address of the J Series device issuing the traceroute monitor command.
psize <i>size</i>	Size of ping request packet, in bytes.
Keys	

Table 211: CLI traceroute monitor Command Output Summary (*continued*)

Field	Description
Help	Displays the help for the CLI commands. Press H to display the help.
Display mode	Toggles the display mode. Press D to toggle the display mode
Restart statistics	Restarts the traceroute monitor command. Press R to restart the traceroute monitor command.
Order of fields	Sets the order of the displayed fields. Press O to set the order of the displayed fields.
quit	Quits the traceroute monitor command. Press Q to quit the traceroute monitor command.
Packets	
<i>number</i>	Number of the hop (router) along the route to the final destination host.
Host	Hostname or IP address of the router at each hop.
Loss%	Percent of packet loss. The number of ping responses divided by the number of ping requests, specified as a percentage.
Pings	
Snt	Number of ping requests sent to the router at this hop.
Last	Most recent round-trip time, in milliseconds, to the router at this hop.
Avg	Average round-trip time, in milliseconds, to the router at this hop.
Best	Shortest round-trip time, in milliseconds, to the router at this hop.
Wrst	Longest round-trip time, in milliseconds, to the router at this hop.
StDev	Standard deviation of round-trip times, in milliseconds, to the router at this hop.

Tracing Multicast Routes from the CLI

Use CLI **mtrace** commands to trace information about multicast paths. The **mtrace from-source** command displays information about a multicast path from a source to the J Series device. The **mtrace monitor** command monitors and displays multicast trace operations.

This section contains the following topics. For more information about **mtrace** commands, see the *JUNOS System Basics and Services Command Reference*.

- Using the **mtrace from-source** Command on page 370
- Using the **mtrace monitor** Command on page 372

Using the mtrace from-source Command

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. Table 212 on page 370 describes the **mtrace from-source** command options.

```
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 212: CLI mtrace from-source Command Options

Option	Description
source <i>host</i>	Traces the path to the specified hostname or IP address.
extra-hops <i>number</i>	(Optional) Sets the number of extra hops to trace past nonresponsive routers. Specify a value from 0 through 255.
group <i>address</i>	(Optional) Traces the path for the specified group address. The default value is 0.0.0.0.
interval <i>seconds</i>	(Optional) Sets the interval between statistics gathering. The default value is 10.
max-hops <i>number</i>	(Optional) Sets the maximum number of hops to trace toward the source. Specify a value from 0 through 255. The default value is 32.
max-queries <i>number</i>	(Optional) Sets the maximum number of query attempts for any hop. Specify a value from 1 through 32. The default value is 3.
response <i>host</i>	(Optional) Sends the response packets to the specified hostname or IP address. By default, the response packets are sent to the J Series device.
routing-instance <i>routing-instance-name</i>	(Optional) Traces the routing instance you specify.
ttl <i>number</i>	(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.
wait-time <i>seconds</i>	(Optional) Sets the time to wait for a response packet. The default value is 3 seconds.
loop	(Optional) Loops indefinitely, displaying rate and loss statistics. To quit the mtrace command, press Ctrl-C.
multicast-response	(Optional) Forces the responses to use multicast.
unicast-response	(Optional) Forces the response packets to use unicast.

Table 212: CLI mtrace from-source Command Options (continued)

Option	Description
no-resolve	(Optional) Does not display hostnames.
no-router-alert	(Optional) Does not use the router alert IP option in the IP header.
brief	(Optional) Does not display packet rates and losses.
detail	(Optional) Displays packet rates and losses if a group address is specified.

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 routers along the path):

hop-number host (ip-address) protocolttl

Table 213 on page 371 summarizes the output fields of the display.



NOTE: The packet statistics gathered from Juniper Networks routers and routing nodes are always displayed as 0.

Table 213: CLI mtrace from-source Command Output Summary

Field	Description
<i>hop-number</i>	Number of the hop (router) along the path.
<i>host</i>	Hostname, if available, or IP address of the router. If the no-resolve option was entered in the command, the hostname is not displayed.
<i>ip-address</i>	IP address of the router.
<i>protocol</i>	Protocol used.
<i>ttl</i>	TTL threshold.

Table 213: CLI mtrace from-source Command Output Summary (continued)

Field	Description
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.

Using the mtrace monitor Command

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. When the device captures an `mtrace` response, the display is similar, but the complete `mtrace` response is also displayed—exactly as it is displayed in `mtrace from-source` command output.

Table 214 on page 372 summarizes the output fields of the display.

Table 214: CLI mtrace monitor Command Output Summary

Field	Description
Mtrace <i>operation-type</i> at <i>time-of-day</i>	<ul style="list-style-type: none"> ■ <i>operation-type</i>—Type of multicast trace operation: <code>query</code> or <code>response</code>. ■ <i>time-of-day</i>—Date and time the multicast trace query or response was captured.
by	IP address of the host issuing the query.
resp to <i>address</i>	<i>address</i> —Response destination address.

Table 214: CLI mtrace monitor Command Output Summary (continued)

Field	Description
qid <i>qid</i>	<i>qid</i> —Query ID number.
packet from <i>source</i> to <i>destination</i>	<ul style="list-style-type: none"> ■ <i>source</i>—IP address of the source of the query or response. ■ <i>destination</i>—IP address of the destination of the query or response.
from <i>source</i> to <i>destination</i>	<ul style="list-style-type: none"> ■ <i>source</i>—IP address of the multicast source. ■ <i>destination</i>—IP address of the multicast destination.
via group <i>address</i>	<i>address</i> —Group address being traced.
mxhop= <i>number</i>	<i>number</i> —Maximum hop setting.

Displaying Log and Trace Files from the CLI

You can 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 is displayed 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.

Monitoring Interfaces and Traffic from the CLI

This section contains the following topics:

- Using the monitor interface Command on page 373
- Using the monitor traffic Command on page 375

Using the monitor interface Command

Use the CLI **monitor interface** command to display real-time traffic, error, alarm, and filter statistics about a physical or logical interface. Enter the command with the following syntax:

```
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 are displayed.

The real-time statistics are updated 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 215 on page 374 and Table 216 on page 374 list the keys you use to control the display using the *interface-name* and *traffic* options. (The keys are not case sensitive.)

Table 215: CLI monitor interface Output Control Keys

Key	Action
c	Clears (returns to 0) the delta counters in the Current delta column. The statistics counters are not cleared.
f	Freezes the display, halting the update of the statistics and delta counters.
i	Displays information about a different interface. You are prompted for the name of a specific interface.
n	Displays information about the next interface. The device scrolls through the physical and logical interfaces in the same order in which they are displayed by the show interfaces terse 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 216: 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 Delta column. The statistics counters are not cleared.
d	Displays the Delta 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 Delta column.

Following are sample displays from the **monitor interface** command:

```

user@host> monitor interface fe-0/0/0
host1                               Seconds: 11                Time: 16:47:49
                                   Delay: 0/0/0
Interface: fe-0/0/0, Enabled, Link is Up Encapsulation: Ethernet, Speed: 100mbps
Traffic statistics:
Input bytes:                       381588589          Current delta
bytes:                             9707279             [11583] Output
                                   [6542] Input

```

```

packets:                4064553                [145] Output
packets:                66683                  [25] Error
statistics:  Input errors:                0
               [0] Input drops:                0
               [0] Input framing errors:        0
               Carrier transitions:            0
Output errors:                0                [0] Output
drops:                      0                [0]

```



NOTE: The output fields displayed 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)

```

Using the monitor traffic Command

Use the CLI `monitor traffic` command to display packet headers transmitted through network interfaces.



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.

Enter the `monitor traffic` command with the following syntax. Table 217 on page 375 describes the `monitor traffic` command options.

```

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>

```

To quit the `monitor traffic` command and return to the command prompt, press Ctrl-C.

If you want to capture and view packet headers using the J-Web interface, see “Capturing and Viewing Packets with the J-Web Interface” on page 354.

Table 217: CLI monitor traffic Command Options

Option	Description
<code>absolute-sequence</code>	(Optional) Displays the absolute TCP sequence numbers.
<code>count number</code>	(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.

Table 217: CLI monitor traffic Command Options (*continued*)

Option	Description
<code>interface interface-name</code>	(Optional) Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.
<code>layer2-headers</code>	(Optional) Displays the link-layer packet header on each line.
<code>matching "expression"</code>	(Optional) Displays packet headers that match an expression enclosed in quotation marks (" "). Table 218 on page 377 through Table 220 on page 379 list match conditions, logical operators, and arithmetic, binary, and relational operators you can use in the expression.
<code>no-domain-names</code>	(Optional) Suppresses the display of the domain name portion of the hostname.
<code>no-promiscuous</code>	(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.
<code>no-resolve</code>	(Optional) Suppresses the display of hostnames.
<code>no-timestamp</code>	(Optional) Suppresses the display of packet header timestamps.
<code>print-ascii</code>	(Optional) Displays each packet header in ASCII format.
<code>print-hex</code>	(Optional) Displays each packet header, except link-layer headers, in hexadecimal format.
<code>size bytes</code>	(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 96 .
<code>brief</code>	(Optional) Displays minimum packet header information. This is the default.
<code>detail</code>	(Optional) Displays packet header information in moderate detail. For some protocols, you must also use the size option to see detailed information.
<code>extensive</code>	(Optional) Displays the most extensive level of packet header information. For some protocols, you must also use the size option to see extensive information.

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 218 on page 377, enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in Table 219 on page 378 (shown in order of highest to lowest precedence).

For example, to display TCP or UDP packet headers, enter the following command:

```
user@host> monitor traffic matching "tcp || udp"
```

To compare the following types of expressions, use the relational operators listed in Table 220 on page 379 (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in Table 220 on page 379.
- Binary—Expressions that use the binary operators listed in Table 220 on page 379.
- Packet data accessor—Expressions that use the following syntax:

```
protocol [byte-offset <size>]
```

Replace *protocol* with any protocol in Table 218 on page 377. 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 218: CLI monitor traffic Match Conditions

Match Condition	Description
Entity Type	
host [<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 host: arp, ip, rarp, or any of the Directional match conditions.
network <i>address</i>	Matches packet headers with source or destination addresses containing the specified network address.
network <i>address</i> mask <i>mask</i>	Matches packet headers containing the specified network address and subnet mask.
port [<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.
Directional	
destination	Matches packet headers containing the specified destination.
source	Matches packet headers containing the specified source.
source and destination	Matches packet headers containing the specified source <i>and</i> destination.
source or destination	Matches packet headers containing the specified source <i>or</i> destination.

Table 218: CLI monitor traffic Match Conditions (*continued*)

Match Condition	Description
Packet Length	
less bytes	Matches packets with lengths less than or equal to the specified value, in bytes.
greater bytes	Matches packets with lengths greater than or equal to the specified value, in bytes.
Protocol	
arp	Matches all ARP packets.
ether	Matches all Ethernet frames.
ether [broadcast multicast]	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with source or destination .
ether protocol [address (\arp \ip \rarp)]	Matches Ethernet frames with the specified address or protocol type. The arguments arp , ip , and rarp are also independent match conditions, so they must be preceded with a backslash (\) when used in the ether protocol match condition.
icmp	Matches all ICMP packets.
ip	Matches all IP packets.
ip [broadcast multicast]	Matches broadcast or multicast IP packets.
ip protocol [address (\icmp igmp \tcp \udp)]	Matches IP packets with the specified address or protocol type. The arguments icmp , tcp , and udp are also independent match conditions, so they must be preceded with a backslash (\) when used in the ip protocol match condition.
isis	Matches all IS-IS routing messages.
rarp	Matches all RARP packets.
tcp	Matches all TCP packets.
udp	Matches all UDP packets.

Table 219: CLI monitor traffic Logical Operators

Logical Operator	Description
!	Logical NOT. If the first condition does not match, the next condition is evaluated.
&&	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 (\).

Table 220: CLI monitor traffic Arithmetic, Binary, and Relational Operators

Operator	Description
Arithmetic Operator	
+	Addition operator.
–	Subtraction operator.
/	Division operator.
Binary Operator	
&	Bitwise AND.
*	Bitwise exclusive OR.
	Bitwise inclusive OR.
Relational Operator	
<=	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.

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
```


Chapter 22

Configuring Packet Capture

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.

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. For more information, see “Capturing and Viewing Packets with the J-Web Interface” on page 354.



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. For more information about packet capture, see the *JUNOS Policy Framework Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- Packet Capture Terms on page 381
- Packet Capture Overview on page 382
- Before You Begin on page 385
- Configuring Packet Capture with a Configuration Editor on page 385
- Changing Encapsulation on Interfaces with Packet Capture Configured on page 390
- Verifying Packet Capture on page 391

Packet Capture Terms

Before configuring packet capture on a device, become familiar with the terms defined in Table 221 on page 382.

Table 221: Packet Capture Terms

Term	Definition
interface sampling	Packet sampling method used by packet capture, in which entire IPv4 packets flowing in the input or output direction, or both directions, are captured for analysis.
libpcap	An implementation of the pcap application programming interface. libpcap may be used by a program to capture packets traveling over a network.
packet capture	<ol style="list-style-type: none"> 1. Packet sampling method in which entire IPv4 packets flowing through a router are captured for analysis. Packets are captured in the Routing Engine and stored as libpcap-formatted files in the <code>/var/tmp</code> directory on the router. Packet capture files can be opened and analyzed offline with packet analyzers such as tcpdump or Ethereal. To avoid performance degradation on the router, implement packet capture with firewall filters that capture only selected packets. <i>See also traffic sampling.</i> 2. Packet sampling method available from the J-Web interface, for capturing the headers of packets destined for or originating from the Routing Engine. (See “Capturing and Viewing Packets with the J-Web Interface” on page 354).
packet loss priority (PLP) bit	Bit used to identify packets that have experienced congestion or are from a transmission that exceeded a service provider's customer service license agreement. This bit can be used as part of a router's congestion control mechanism and can be set by the interface or by a filter.
port mirroring	<p>The process of sending a copy of a packet from the router to an external host address.</p> <p>For more information about port mirroring, see the <i>JUNOS Policy Framework Configuration Guide</i>.</p>
tcpdump	A command line utility for debugging computer network problems. tcpdump allows the user to display the contents of TCP/IP and other packets captured on a network interface. On UNIX and most other operating systems, a user must have superuser privileges to use tcpdump due to its use of promiscuous mode.
traffic sampling	Packet sampling method in which the sampling key based on the IPv4 header is sent to the Routing Engine. There, the key is placed in a file, or cflowd packets based on the key and are sent to a cflowd server for analysis. <i>See also packet capture.</i>

Packet Capture Overview

Packet capture is used by network administrators and security engineers for the following purposes:

- 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 rather than packet headers and saves the contents to a file in the 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.

For more information about traffic sampling, see the *JUNOS Policy Framework Configuration Guide*.

This overview contains the following topics:

- Packet Capture on Device Interfaces on page 383
- Firewall Filters for Packet Capture on page 384
- Packet Capture Files on page 384
- Analysis of Packet Capture Files on page 384

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 output direction.

Tunnel interfaces can support packet capture in the outbound direction only.

Use the J-Web configuration editor or CLI configuration editor to specify maximum packet size, the filename to be used for storing the captured packets, maximum file size, maximum number of packet capture files, and the file permissions. See “Configuring Packet Capture on an Interface (Required)” on page 387.



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. For more information, see “Changing Encapsulation on Interfaces with Packet Capture Configured” on page 390.

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 router, because interface sampling does not capture packets originating from the host router.

To configure firewall filters for packet capture, see “Configuring a Firewall Filter for Packet Capture (Optional)” on page 388.

For more information about firewall filters, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

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, maximum size of the file, and 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-0.0.1.0** 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. To disable packet capture on an interface, see “Disabling Packet Capture” on page 389.

For more details about analyzing packet capture files, see “Verifying Captured Packets” on page 392.

Before You Begin

Before you begin configuring packet capture, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See the *JUNOS Software Interfaces and Routing Configuration Guide*.
- If you do not already have an understanding of the packet capture feature, see “Packet Capture Overview” on page 382.

Configuring Packet Capture with a Configuration Editor

To configure packet capture on a device, you must perform the following tasks marked *(Required)*:

- Enabling Packet Capture (Required) on page 385
- Configuring Packet Capture on an Interface (Required) on page 387
- Configuring a Firewall Filter for Packet Capture (Optional) on page 388
- Disabling Packet Capture on page 389
- Deleting Packet Capture Files on page 389

Enabling Packet Capture (Required)

To enable packet capture on the device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 222 on page 386.
3. Go on to “Configuring Packet Capture on an Interface (Required)” on page 387.

Table 222: Enabling Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Forwarding options level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Forwarding options, click Configure or Edit. 3. Next to Scripts, click Configure or Edit. 4. Next to Commits, click Configure or Edit. <p>In the configuration editor hierarchy, select Forwarding options.</p>	<p>From the [edit] hierarchy level, enter</p> <pre>edit forwarding-options</pre>
Specify in bytes the maximum size of each packet to capture in each file—for example, 500. The range is between 68 and 1500, and the default is 68 bytes.	<ol style="list-style-type: none"> 1. From the Sampling or packet capture list, select Packet capture. 2. Next to Packet capture, click Configure. 3. In the Maximum capture size box, type 500. 	<p>Enter</p> <pre>set packet-capture maximum-capture-size 500</pre>
<p>Specify the target filename for the packet capture file—for example, pcap-file. For each physical interface, the interface name is automatically suffixed to the filename—for example, pcap-file.fe-0.0.1.</p> <p>(See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i>.)</p>	In the Filename box, type pcap-file .	<p>Enter</p> <pre>set packet-capture file filename pcap-file</pre>
Specify the maximum number of files to capture—for example, 100. The range is between 2 and 10,000, and the default is 10 files.	In the Files box, type 100.	<p>Enter</p> <pre>set packet-capture file files 100</pre>
Specify the maximum size of each file in bytes—for example, 1024. The range is between 1,024 and 104,857,600, and the default is 512,000 bytes.	In the Size box, type 1024.	<p>Enter</p> <pre>set packet-capture file size 1024</pre>
Specify if all users have permission to read the packet capture files.	<ol style="list-style-type: none"> 1. Next to World readable, select Yes. 2. Click OK. 	<p>Enter</p> <pre>set packet-capture file world-readable</pre>

Configuring Packet Capture on an Interface (Required)

To capture all transit and host-bound packets on an interface and specify the direction of the traffic to capture—inbound, outbound, or both:

- 1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- 2. Perform the configuration tasks described in Table 223 on page 387.
- 3. If you are finished configuring the device, commit the configuration.
- 4. Go on to one of the following procedures:
 - To configure a firewall filter, see “Configuring a Firewall Filter for Packet Capture (Optional)” on page 388.
 - To check the configuration, see “Verifying Packet Capture” on page 391.

Table 223: Configuring Packet Capture on an Interface

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Interfaces level in the configuration hierarchy, and select an interface for packet capture—for example, fe-0/0/1. (See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i> .)	<ul style="list-style-type: none">1. In the J-Web interface, select CLI Tools > Point and Click CLI.2. Next to Interfaces, click Configure or Edit.3. In the Interface name box, click fe-0/0/1.	From the [edit] hierarchy level, enter edit interfaces fe-0/0/1
Configure the direction of the traffic for which you are enabling packet capture on the logical interface—for example, inbound and outbound.	<ul style="list-style-type: none">1. In the Interface unit number box, click 0.2. Next to Inet, select Yes, and click Edit.3. Next to Sampling, click Configure.4. Next to Input, select Yes.5. Next to Output, select Yes.6. Click OK until you return to the Interface page.	Enter set unit 0 family inet sampling input output



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.

Configuring a Firewall Filter for Packet Capture (Optional)

To configure a firewall filter and apply it to the logical interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 224 on page 388.
3. If you are finished configuring the device, commit the configuration.
4. To check the configuration, see “Verifying Packet Capture” on page 391.

Table 224: Configuring a Firewall Filter for Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Firewall level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Firewall, click Configure or Edit. 	From the [edit] hierarchy level, enter edit firewall
Define a firewall filter dest-all and a filter term—for example, dest-term —to capture packets with a particular destination address—for example, 192.168.1.1/32 .	<ol style="list-style-type: none"> 1. Next to Filter, click Add new entry. 2. In the filter name box, type dest-all. 3. Next to Term, click Add new entry. 4. In the Rule name box, type dest-term. 5. Next to From, click Configure. 6. Next to Destination address, click Add new entry. 7. In the Address box, type 192.168.1.1/32. 8. Click OK until you return to the Configuration page. 	Set the filter and term name, and define the match condition and its action. 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
Navigate to the Interfaces level in the configuration hierarchy.	In the configuration editor hierarchy, select Interfaces .	Enter
Apply the dest-all filter to all the outgoing packets on the interface—for example, fe-0/0/1.0 . (See the interface naming conventions in the <i>JUNOS Software Interfaces and Routing Configuration Guide</i> .)	<ol style="list-style-type: none"> 1. In the Interface name box, click fe-0/0/1. 2. In the Interface unit number box, click 0. 3. Next to Inet, select Yes, and click Edit. 4. Next to Filter, click Configure. 5. In the Output box, type dest-all. 6. Click OK until you return to the Interfaces page. 	set interfaces fe-0/0/1 unit 0 family inet filter output dest-all



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.

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:

- 1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- 2. Perform the configuration tasks described in Table 225 on page 389.
- 3. If you are finished configuring the device, commit the configuration.

Table 225: Disabling Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Forwarding options level in the configuration hierarchy.	<ul style="list-style-type: none">1. In the J-Web interface, select CLI Tools > Point and Click CLI.2. Next to Forwarding options, click Configure or Edit.	From the [edit] hierarchy level, enter <code>edit forwarding-options</code>
Disable packet capture.	<ul style="list-style-type: none">1. Next to Packet capture, click Edit.2. Next to Disable, select Yes.3. Click OK until you return to the Configuration page.	Enter <code>set packet-capture disable</code> .

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. You must follow the procedure given in this section to delete packet capture files.

To delete a packet capture file:

- 1. Disable packet capture following the steps in “Disabling Packet Capture” on page 389.
- 2. Using the CLI, delete the packet capture file for the interface:
 - a. From CLI 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 the CLI operational mode:

```
% exit
user@host>
```

3. Reenable packet capture following the steps in “Enabling Packet Capture (Required)” on page 385.
4. Commit the configuration.

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 router.

To change the encapsulation on packet capture-configured interfaces:

1. Disable packet capture following the steps in “Disabling Packet Capture” on page 389.
2. Commit the configuration.
3. Using the CLI, rename the latest packet capture file on which you are changing the encapsulation, with the `.chdsl` extension:
 - a. From CLI 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 the CLI operational mode:

```
% exit
user@host>
```

4. Change the encapsulation on the interface using the J-Web or CLI configuration editor.

See instructions for configuring interfaces in the *JUNOS Software Interfaces and Routing Configuration Guide*

5. Commit the configuration.
6. Reenable packet capture following the steps in “Enabling Packet Capture (Required)” on page 385.
7. Commit the configuration.

Verifying Packet Capture

To verify packet capture, perform these tasks:

- Displaying a Packet Capture Configuration on page 391
- Displaying a Firewall Filter for Packet Capture Configuration on page 392
- Verifying Captured Packets on page 392

Displaying a Packet Capture Configuration

Purpose Verify the packet capture configuration.

Action From the J-Web interface, select **CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the `show forwarding-options` command.

```
[edit]
user@host# show forwarding-options
packet-capture {
  file filename pcap-file files 100 size 1024;
  maximum-capture-size 500;
}
```

Meaning Verify that the output shows the intended file configuration for capturing packets.

Related Topics For more information about the format of a configuration file, see the information about viewing configuration text in the *J-Web Interface User Guide* or the *JUNOS CLI User Guide*.

Displaying a Firewall Filter for Packet Capture Configuration

Purpose Verify the firewall filter for packet capture configuration.

Action From the J-Web interface, select **CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the `show firewall filter dest-all` command.

```
[edit]
user@host# show firewall filter dest-all
term dest-term {
  from {
    destination-address 192.168.1.1/32;
  }
  then {
    sample;
    accept;
  }
}
```

Meaning Verify that the output shows the intended configuration of the firewall filter for capturing packets sent to the destination address 192.168.1.1/32.

Related Topics For more information about the format of a configuration file, see the information about viewing configuration text in the *JUNOS CLI User Guide*.

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 Take the following actions:

- Disable packet capture. See “Disabling Packet Capture” on page 389.
- Perform these steps to 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`), using FTP.

1. From the CLI configuration mode, connect to `tools-server` using FTP:

```
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>
```

2. Navigate to the directory where packet capture files are stored on the device:

```
ftp> lcd /var/tmp
```

Local directory now /cf/var/tmp

3. Copy the packet capture file that you want to analyze—for example, 126b.fe-0.0.1, to the server:

```
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)
```

4. Return to the CLI configuration mode:

```
ftp> bye
221 Goodbye.
[edit]
user@host#
```

- Open the packet capture file on the server with tcpdump or any packet analyzer that supports libpcap format.

Sample Output

```
root@server% tcpdump -r 126b.fe-0.0.1 -xevvvv
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%
```

Meaning Verify that the output shows the intended packets.

Chapter 23

Configuring RPM Probes

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.

For more information about RPM, see the *JUNOS Services Interfaces Configuration Guide*.

For information about which devices support the features documented in this chapter, see “Support Overview for Administration Features” on page 1.

This chapter contains the following topics.

- RPM Terms on page 395
- RPM Overview on page 396
- Before You Begin on page 399
- Configuring RPM with Quick Configuration on page 400
- Configuring RPM with a Configuration Editor on page 406
- Verifying an RPM Configuration on page 415
- Monitoring RPM Probes on page 418

RPM Terms

Before configuring and monitoring RPM, become familiar with the terms defined in Table 226 on page 395.

Table 226: RPM Terms

Term	Definition
egress	Outbound. Characterizing packets exiting a device.
ingress	Inbound. Characterizing packets entering a device.
jitter	Difference in relative transmit time between two consecutive packets in a stream, which can cause quality degradation in some real-time applications such as voice over IP (VoIP) and video.
probe	An action taken or an object used to learn something about the state of the network. Real-time performance monitoring (RPM) uses several types of requests to probe a network.

Table 226: RPM Terms (*continued*)

Term	Definition
probe interval	Time, in seconds, between probe packets.
real-time performance monitoring (RPM)	Monitoring tool that measures the performance of a network between two endpoints by collecting statistics on packet loss, round-trip time, and jitter.
RPM target	Remote network endpoint, identified by an IP address or URL, to which the device sends a real-time performance monitoring (RPM) probe.
RPM test	A collection of real-time performance monitoring (RPM) probes sent out at regular intervals.
test interval	Time, in seconds, between RPM tests.

RPM Overview

Real-time performance monitoring (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 396
- RPM Tests on page 397
- Probe and Test Intervals on page 397
- Jitter Measurement with Hardware Timestamping on page 397
- RPM Statistics on page 398
- RPM Thresholds and Traps on page 399
- RPM for BGP Monitoring on page 399

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. To configure SNMP, see “Configuring SNMP for Network Management” on page 85.

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. To configure SNMP, see “Configuring SNMP for Network Management” on page 85.

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 shown in Table 227 on page 398.

Table 227: RPM Statistics

RPM Statistics	Description
Round-Trip Times	
Minimum round-trip time	Shortest round-trip time from the J Series or SRX Series device to the remote server, as measured over the course of the test
Maximum round-trip time	Longest round-trip time from the J Series or SRX Series device to the remote server, as measured over the course of the test
Average round-trip time	Average round-trip time from the J Series or SRX Series 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 J Series or SRX Series device to the remote server, as measured over the course of the test
Jitter	Difference between the maximum and minimum round-trip times, as measured over the course of the test
Inbound and Outbound Times (ICMP Timestamp Probes Only)	
Minimum egress time	Shortest one-way time from the J Series or SRX Series 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 J Series or SRX Series device, as measured over the course of the test
Average egress time	Average one-way time from the J Series or SRX Series 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 J Series or SRX Series device, as measured over the course of the test
Standard deviation egress time	Standard deviation of the one-way times from the J Series or SRX Series 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 J Series or SRX Series 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

Table 227: RPM Statistics *(continued)*

RPM Statistics	Description
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
Probe Counts	
Probes sent	Total number of probes sent over the course of the test
Probe responses received	Total number of probe responses received over the course of the test
Loss percentage	Percentage of probes sent for which a response was not received

RPM Thresholds and Traps

You can configure RPM threshold values for the round-trip times, ingress (inbound) times, and egress (outbound) times that are measured for each probe, as well as for the standard deviation and jitter values that are measured for each test. Additionally, you can configure threshold values for the number of successive lost probes within a test and the total number of lost probes within a test.

If the result of a probe or test exceeds any threshold, the device generates a system log message and sends any Simple Network Management Protocol (SNMP) notifications (traps) that you have configured.

RPM for BGP Monitoring

When managing peering networks that are connected using Border Gateway Protocol (BGP), you might need to find out if a path exists between the J Series or SRX Series 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.

For BGP configuration information, see the *JUNOS Software Interfaces and Routing Configuration Guide*.

Before You Begin

Before you begin configuring RPM, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See the *JUNOS Software Interfaces and Routing Configuration Guide*.
- Configure SNMP. See “Configuring SNMP for Network Management” on page 85.

Configuring RPM with Quick Configuration

J-Web Quick Configuration allows you to configure real-time performance monitoring (RPM) parameters. Figure 26 on page 400 shows the main Quick Configuration page for RPM. Figure 27 on page 401 shows the probe test Quick Configuration page for RPM.

Figure 26: Main Quick Configuration Page for RPM

Configuration > Quick Configuration > Realtime Performance Monitoring

Quick Configuration

Realtime Performance Monitoring

Probe Owners

No performance probe owners are defined.

Maximum Number of Concurrent Probes

Maximum Number of Concurrent Probes

Probe Servers

TCP Probe Server

UDP Probe Server

Figure 27: Probe Test Quick Configuration Page for RPM

[Configuration](#) > [Quick Configuration](#) > [RPM](#)

Quick Configuration

RPM **Add a Probe Test**

Identification

• Test Name

• Target (Address or URL)

Source Address

Routing Instance ?

History Size ? (50)

Request Information

• Probe Type

Interval ?

• Test Interval ?

Probe Count ?

Destination Port ?

DSCP Bits ?

Data Size ?

Data Fill ?

Hardware Timestamp ☐ ?

Maximum Probe Thresholds

Successive Lost Probes ?

Lost Probes ?

Round Trip Time ?

To configure RPM parameters with Quick Configuration:

1. In the J-Web interface, select **Troubleshoot > RPM > Setup RPM**.
2. Enter information into the Quick Configuration page for RPM, as described in Table 228 on page 402.
3. From the main RPM Quick Configuration page, click one of the following buttons:
 - To apply the configuration and stay on the Quick Configuration RPM page, click **Apply**.
 - To apply the configuration and return to the Quick Configuration main page, click **OK**.
 - To cancel your entries and return to the Quick Configuration RPM page, click **Cancel**.
4. To check the configuration, see “Verifying an RPM Configuration” on page 415.

Table 228: RPM Quick Configuration Summary

Field	Function	Your Action
Performance Probe Owners		
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.
Identification		
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 <code>http://</code> .
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 <code>icmp</code> and <code>icmp-timestamp</code> . The default routing instance is <code>inet.0</code> .
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.
Request Information		
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"> ■ <code>http-get</code> ■ <code>http-get-metadata</code> ■ <code>icmp-ping</code> ■ <code>icmp-ping-timestamp</code> ■ <code>tcp-ping</code> ■ <code>udp-ping</code>
Interval	Sets the wait time (in seconds) between each probe transmission	Type a number between 1 and 255 (seconds).
Test Interval (required)	Sets the wait time (in seconds) between tests.	Type a number between 0 and 86400 (seconds).
Probe Count	Sets the total number of probes to be sent for each test.	Type a number between 1 and 15.

Table 228: RPM Quick Configuration Summary (continued)

Field	Function	Your Action
Destination Port	<p>Specifies the TCP or UDP port to which probes are sent.</p> <p>To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks devices configured to receive and transmit RPM probes on the same TCP or UDP port.</p>	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	<p>Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern. The default is 000000.</p> <p>For information about DSCPs and their use within class-of-service (CoS) features, see the <i>JUNOS Software Interfaces and Routing Configuration Guide</i>.</p>	Type a valid 6-bit pattern.
Data Size	Specifies the size of the data portion of the ICMP probes.	Type a size (in bytes) between 0 and 65507.
Data Fill	Specifies the contents of the data portion of the ICMP probes.	Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.
Hardware Timestamp	<p>Enables timestamping of RPM probe messages. You can timestamp the following RPM probes to improve the measurement of latency or jitter:</p> <ul style="list-style-type: none"> ■ ICMP ping ■ ICMP ping timestamp ■ UDP ping—destination port UDP-ECHO (port 7) only ■ UDP ping timestamp—destination port UDP-ECHO (port 7) only 	To enable timestamping, select the check box.
Maximum Probe Thresholds		
Successive Lost Probes	Sets the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Lost Probes	Sets the total number of probes that must be lost to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Round Trip Time	Sets the total round-trip time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter	Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).

Table 228: RPM Quick Configuration Summary *(continued)*

Field	Function	Your Action
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Sets the total one-way time (in microseconds), from the device to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Ingress Time	Sets the total one-way time (in microseconds), from the remote server to the device, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds)
Jitter Egress Time	Sets the total outbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds)
Jitter Ingress Time	Sets the total inbound-time jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Standard Deviation	Sets the maximum allowable standard deviation of outbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Ingress Standard Deviation	Sets the maximum allowable standard deviation of inbound times (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Traps		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.

Table 228: RPM Quick 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"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Ingress Time Exceeded	Generates traps when the threshold for maximum inbound time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Jitter Exceeded	Generates traps when the threshold for jitter in round-trip time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Probe Failure	Generates traps when the threshold for the number of successive lost probes is reached.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
RTT Exceeded	Generates traps when the threshold for maximum round-trip time is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Standard Deviation Exceeded	Generates traps when the threshold for standard deviation in round-trip times is exceeded.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Test Completion	Generates traps when a test is completed.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Test Failure	Generates traps when the threshold for the total number of lost probes is reached.	<ul style="list-style-type: none"> ■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Performance Probe Server		
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.

Configuring RPM with a Configuration Editor

To configure the device to perform real-time performance tests, you perform the following tasks. For information about using the J-Web and CLI configuration editors, see “User Interface Overview” on page 23.

- Configuring Basic RPM Probes on page 406
- Configuring TCP and UDP Probes on page 409
- Tuning RPM Probes on page 411
- Configuring RPM Probes to Monitor BGP Neighbors on page 412

Configuring Basic RPM Probes

To configure basic RPM probes, you must configure the probe owner, the test, and the specific parameters of the RPM probe.

For ICMP ping, ICMP ping timestamp, UDP ping, and UDP ping timestamp probes, you can also set a timestamp to improve the measurement of latency or jitter. The probe is timestamped by the device originating the probe (the RPM client).

In this sample use of RPM, basic probes are configured for two customers: Customer A and Customer B. The probe for Customer A uses ICMP timestamp packets and sets RPM thresholds and corresponding SNMP traps to catch lengthy inbound times. The probe for Customer B uses HTTP packets and sets thresholds and corresponding SNMP traps to catch excessive lost probes. To configure these RPM probes:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 229 on page 407.
3. If you are finished configuring the network, commit the configuration.
4. Go on to one of the following procedures:
 - To configure a TCP or UDP probe, see “Configuring TCP and UDP Probes” on page 409.
 - To tune a probe, see “Tuning RPM Probes” on page 411.
 - To check the configuration, see “Verifying an RPM Configuration” on page 415.

Table 229: Configuring Basic RPM Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Services > RPM level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box. 4. Click Configure. 	<p>From the [edit] hierarchy level, enter</p> <pre>edit services rpm</pre>
Configure the RPM owners customerA and customerB .	<ol style="list-style-type: none"> 1. In the Probe box, click Add new entry. 2. In the Owner box, type customerA. 3. Click OK. 4. Repeat the previous steps and add an RPM probe owner for customerB. 	<ol style="list-style-type: none"> 1. Enter set probe customerA 2. Enter set probe customerB
<p>Configure the RPM test icmp-test for the RPM owner customerA.</p> <p>The sample RPM test is an ICMP probe with a test interval (probe frequency) of 15 seconds, a probe type of icmp-ping-timestamp, a probe timestamp, and a target address of 192.178.16.5.</p>	<ol style="list-style-type: none"> 1. On the Rpm page, select customerA. 2. In the Test box, click Add new entry 3. In the Name box, type icmp-test. 4. In the Test interval box, type 15. 5. In the Probe type box, select icmp-ping-timestamp. 6. Select the Hardware timestamp check box. 7. In the Target box, select the Yes check box, and click Configure. 8. In the Target type box, select Address. 9. In the Address box, type 192.178.16.5. 10. Click OK. 	<ol style="list-style-type: none"> 1. From the [edit] hierarchy level, enter edit services rpm probe customerA 2. Enter set test icmp-test probe-frequency 15 3. Enter set test icmp-test probe-type icmp-ping-timestamp 4. Enter set test icmp-test hardware-timestamp 5. Enter set test icmp-test target address 192.178.16.5

Table 229: Configuring Basic RPM Probes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.	<ol style="list-style-type: none"> 1. On the Probe page, select icmp-test. 2. In the Thresholds box, select the Yes check box, and click Configure. 3. In the Ingress time box, type 3000. 4. Click OK. 5. In the Traps box, click Add new entry. 6. In the Value box, select ingress-time-exceeded. 7. Click OK. 	<ol style="list-style-type: none"> 1. Enter set probe customerA test icmp-test thresholds ingress-time 3000 2. Enter set probe customerA test icmp-test traps ingress-time-exceeded
<p>Configure the RPM test http-test for the RPM owner customerB.</p> <p>The sample RPM test is an HTTP probe with a test interval (probe frequency) of 30 seconds, a probe type of http-get, and a target URL of http://customerB.net.</p>	<ol style="list-style-type: none"> 1. On the Rpm page, select customerB. 2. In the Test box, click Add new entry. 3. In the Name box, type http-test. 4. In the Test interval box, type 30. 5. In the Probe type box, select http-get. 6. In the Target box, select the Yes check box, and click Configure. 7. In the Target type box, select Url. 8. In the Url box, type http://customerB.net. 9. Click OK. 	<ol style="list-style-type: none"> 1. From the [edit] hierarchy level, enter edit services rpm probe customerB 2. Enter set test http-test probe-frequency 30 3. Enter set test http-test probe-type http-get 4. Enter set test http-test target url http://customerB.net

Table 229: Configuring Basic RPM Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure RPM thresholds and corresponding SNMP traps to catch 3 or more successive lost probes and total lost probes of 10 or more.	1. On the Probe page, select http-test .	1. Enter
	2. In the Thresholds box, select the Yes check box, and click Configure .	set probe customerB test icmp-test thresholds successive-loss 3
	3. In the Successive loss box, type 3.	2. Enter
	4. In the Total loss box, type 10.	set probe customerB test icmp-test thresholds total-loss 10
	5. Click OK .	3. Enter
	6. In the Traps box, click Add new entry .	set probe customerB test icmp-test traps probe-failure
	7. In the Value box, select probe-failure .	4. Enter
	8. Click OK .	set probe customerB test icmp-test traps test-failure
	9. In the Traps box, click Add new entry .	
	10. In the Value box, select test-failure .	
	11. Click OK .	

Configuring TCP and UDP Probes

To configure RPM using TCP and UDP probes, in addition to the basic RPM properties, you must configure both the host device and the remote device to act as TCP and UDP servers.

If you are using class of service (CoS) and want to classify probes, you must also set a destination interface. The destination interface is the output interface for sending packets to the forwarding plane. Classified packets are sent to the output queue on the output interface specified by the CoS scheduler map configured on the interface.

For information about CoS, see the *JUNOS Software Interfaces and Routing Configuration Guide*.



CAUTION: Use probe classification with caution, because improper configuration can cause packets to be dropped.

The destination interface must support looping of probe packets to an input interface without adding any encapsulation. The device's destination interface must be an It services interface.

In this sample use of RPM, a probe is configured for one customer: Customer C. The probe for Customer C uses TCP packets. The remote device is configured as an RPM server for both TCP and UDP packets, using an It services interface as the destination

interface, and ports 50000 and 50037, respectively. Router A is the host device in this example, and Router B is the remote device. To configure this RPM probe:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 230 on page 410.
3. If you are finished configuring the network, commit the configuration.
4. Go on to one of the following procedures:
 - To tune a probe, see “Tuning RPM Probes” on page 411.
 - To check the configuration, see “Verifying an RPM Configuration” on page 415.

Table 230: Configuring TCP and UDP Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Router A Configuration		
Navigate to the Services > RPM level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box. 4. Click Configure. 	<p>From the [edit] hierarchy level, enter</p> <pre>edit services rpm</pre>
Configure the RPM owner customerC .	<ol style="list-style-type: none"> 1. In the Probe box, click Add new entry. 2. In the Owner box, type customerC. 3. Click OK. 	<p>Enter</p> <pre>set probe customerC</pre>
Configure the RPM test tcp-test for the RPM owner customerC . The sample RPM test is a TCP probe with a test interval (probe frequency) of 5, a probe type of tcp-ping , and a target address of 192.162.45.6.	<ol style="list-style-type: none"> 1. On the Rpm page, select customerC. 2. In the Test box, click Add new entry. 3. In the Name box, type tcp-test. 4. In the Test interval box, type 5. 5. In the Probe type box, select tcp-ping. 6. In the Target box, select the Yes check box, and click Configure. 7. In the Target type box, select Address. 8. In the Address box, type 192.162.45.6. 9. Click OK. 	<ol style="list-style-type: none"> 1. From the [edit] hierarchy level, enter edit services rpm probe customerC 2. Enter set test tcp-test probe-frequency 5 3. Enter set test tcp-test probe-type tcp-ping 4. Enter set test tcp-test target address 192.162.45.6

Table 230: Configuring TCP and UDP Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the destination interface. NOTE: On J Series devices, the destination interface must be an It services interface.	In the Destination interface box, type It-0/0/0	Enter set test tcp-test destination-interface It-0/0/0
Configure port 50000 as the TCP port to which the RPM probes are sent.	In the Destination port box, type 50000.	Enter set test tcp-test destination-port 50000
Router B Configuration		
Navigate to the Services > RPM level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box. 4. Click Configure. 	From the [edit] hierarchy level, enter edit services rpm
Configure Router B to act as a TCP server, using port 50000 to send and receive TCP probes.	<ol style="list-style-type: none"> 1. Next to Probe server, click Configure. 2. In the Tcp box, click Configure. 3. In the Port box, type 50000. 4. Click OK. 	Enter set probe-server tcp port 50000
Configure Router B to act as a UDP server, using port 50037 to send and receive UDP probes.	<ol style="list-style-type: none"> 1. Next to Probe server, click Edit. 2. In the Udp box, click Configure. 3. In the Port box, type 50037. 4. Click OK. 	Enter set probe-server udp port 50037

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. This example tunes the ICMP probe set for customer A in “Configuring Basic RPM Probes” on page 406.

To configure tune RPM probes:

1. Perform the configuration tasks described in Table 229 on page 407.
2. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
3. Perform the configuration tasks described in Table 231 on page 412.

4. If you are finished configuring the network, commit the configuration.
5. To check the configuration, see “Verifying an RPM Configuration” on page 415.

Table 231: Tuning RPM Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Services > RPM level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box. 4. Click Edit. 	From the [edit] hierarchy level, enter edit services rpm
Set the maximum number of concurrent probes allowed on the system to 10 .	<ol style="list-style-type: none"> 1. In the Probe limit box, type 10. 2. Click OK. 	Enter set probe-limit 10
Access the ICMP probe of customer A.	<ol style="list-style-type: none"> 1. In the Owner box, click CustomerA. 2. In the Name box, click icmp-test. 	From the [edit] hierarchy level, enter edit services rpm probe customerA test icmp-test
Set the time between probe transmissions to 15 seconds.	In the Probe interval box, type 15 .	Enter set probe-interval 15
Set the number of probes within a test to 10 .	In the Probe count box, type 10 .	Enter set probe-count 10
Set the source address for each probe packet to 192.168.2.9 .	<ol style="list-style-type: none"> 1. In the Source address box, type 192.168.2.9. 2. Click OK. 	Enter set source-address 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.		

Configuring RPM Probes to Monitor BGP Neighbors

By default, the device is not configured to send RPM probes to its BGP neighbors. You must configure the BGP parameters under RPM configuration to send RPM probes to BGP neighbors.

You can also direct the probes to a particular group of BGP neighbors.

This section contains the following topics:

- Configuring RPM Probes for BGP Monitoring on page 413
- Directing RPM Probes to Select BGP Routers on page 414

Configuring RPM Probes for BGP Monitoring

This sample use of RPM for BGP monitoring uses a TCP probe. To use TCP or UDP probes, you must configure both the probe server (J Series or SRX Series device) and the probe receiver (the remote device) to transmit and receive RPM probes on the same TCP or UDP port. The sample probe uses TCP port 50000.

To configure RPM probes on a device to monitor BGP neighbors with a configuration editor:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 232 on page 413.
3. If you are finished configuring the device, commit the configuration.
4. Go on to one of the following tasks:
 - To send probes to specific devices, see “Directing RPM Probes to Select BGP Routers” on page 414.
 - To check the configuration, see “Verifying an RPM Configuration” on page 415.

Table 232: Configuring RPM Probes to Monitor BGP Neighbors

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Services > RPM > BGP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box and click Configure or Edit. 4. Next to Bgp, click Configure. 	From the [edit] hierarchy level, enter edit services rpm bgp
Specify a hexadecimal value (the range is between 1 and 2048 characters) that you want to use for the data portion of the RPM probe—for example, ABCD123.	In the Data fill box, type ABCD123.	Enter set data-fill ABCD123
Specify the data size of the RPM probe in bytes, a value from 0 through 65507—for example, 1024.	In the Data size box, type 1024.	Enter set data-size 1024
Configure port 50000 as the TCP port to which the RPM probes are sent.	In the Destination port box, type 50000.	Enter set destination-port 50000

Table 232: Configuring RPM Probes to Monitor BGP Neighbors *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Specify the number of probe results to be saved in the probe history—for example, 25. The range is between 0 and 255, and the default is 50.	In the History size box, type 25.	Enter set history-size 25
Configure the probe count—for example, 5—and probe interval—for example, 1. <ul style="list-style-type: none"> ■ Probe count—Total number of RPM probes to be sent for each test. The range is between 1 and 15 and the default is 1. ■ Probe interval—Wait time (in seconds) between RPM probes. The range is between 1 and 255, and the default is 3. 	<ol style="list-style-type: none"> In the Probe count box, type 5. In the Probe interval box, type 1. 	Enter set probe-count 5 probe-interval 1
Specify the type of probe to be sent as part of the test— tcp-ping . NOTE: If you do not specify the probe type the default ICMP probes are sent.	In the Probe type box, select tcp-ping .	Enter set probe-type tcp-ping
Configure a value between 0 and 86400 seconds for the interval between tests—for example, 60.	<ol style="list-style-type: none"> In the Test interval box, type 60. Click OK. 	Enter set test-interval 60

Directing RPM Probes to Select BGP Routers

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 routers to receive RPM probes, you can configure routing instances.

The sample RPM configuration in Table 233 on page 415 sends RPM probes to the BGP neighbors in routing instance R1.

To direct RPM probes to select BGP neighbors:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 233 on page 415.
3. If you are finished configuring the device, commit the configuration.
4. To verify the configuration, see “Verifying an RPM Configuration” on page 415.

Table 233: Directing RPM Probes to Select BGP Routers

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Services > RPM > BGP level in the configuration hierarchy.	<ol style="list-style-type: none"> 1. In the J-Web interface, select CLI Tools > Point and Click CLI. 2. Next to Services, click Configure or Edit. 3. Next to Rpm, select the Yes check box and click Configure or Edit. 4. Next to Bgp, click Configure or Edit. 	From the [edit] hierarchy level, enter edit services rpm bgp
Configure routing instance RI1 to send RPM probes to BGP neighbors within the routing instance.	<ol style="list-style-type: none"> 1. Next to Routing instances, click Add new entry. 2. In the Routing instance name box, type RI1. 3. Click OK. 	Enter set routing-instances RI1

Verifying an RPM Configuration

To verify an RPM configuration, perform these tasks:

- Verifying RPM Services on page 415
- Verifying RPM Statistics on page 416
- Verifying RPM Probe Servers on page 417

Verifying RPM Services

Purpose Verify that the RPM configuration is within the expected values.

Action From configuration mode in the CLI, enter the `show services rpm` command.

Sample Output

```

user@host# show services rpm
probe test {
  test customerA {
    probe-type icmp-ping;
    target address 192.178.16.5;
    probe-count 15;
    probe-interval 1;
    hardware-timestamp;
  }
  test customerB {
    probe-type icmp-ping-timestamp;
    target address 192.178.16.5;
    probe-count 15;
    probe-interval 1;
    hardware-timestamp;
  }
  test customerC {
    probe-type udp-ping;
    target address 192.178.16.5;
    probe-count 15;
  }
}

```

```

        probe-interval 1;
        destination-port 50000;
        hardware-timestamp;
    }
}

```

Meaning 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 the J-Web interface, select **Troubleshoot > RPM > View RPM**. From the CLI, enter the `show services rpm probe-results` command.

Sample Output

```

user@host> show services rpm probe-results
Owner: customerA, 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: customerB, 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

```

Meaning The output shows the probe results for the RPM tests configured on the device. Verify the following information:

- Each configured test is displayed. Results are displayed in alphabetical order, sorted first by owner name and then by test name.
- The round-trip times fall within the expected values for the particular test. The minimum round-trip time is displayed as **Minimum Rtt**, the maximum round-trip time is displayed as **Maximum Rtt**, and the average round-trip time is displayed as **Average Rtt**.

A high average round-trip time might mean that performances problems exist within the network. A high maximum round-trip time might result in high jitter values.

- The egress (outbound) trip times fall within the expected values for the particular test. The minimum outbound time is displayed as **Minimum egress time**, the maximum outbound time is displayed as **Maximum egress time**, and the average outbound time is displayed as **Average egress time**.
- The ingress (inbound) trip times fall within the expected values for the particular test. The minimum inbound time is displayed as **Minimum ingress time**, the maximum inbound time is displayed as **Maximum ingress time**, and the average inbound time is displayed as **Average ingress time**.
- The number of probes sent and received is expected.

Lost probes might indicate packet loss through the network. Packet losses can occur if the remote server is flapping. If the RPM probe type is TCP or UDP, complete probe loss might indicate a mismatch in TCP or UDP RPM port number.

- For **Type**, each peer is configured as the correct type (either internal or external).

Related Topics For a complete description of `show services rpm probe-results` output, see the *JUNOS System Basics and Services Command Reference*.

Verifying RPM Probe Servers

Purpose Verify that the device is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

Action From the CLI, enter the `show services rpm active-servers` command.

Sample Output

```
user@host> show services rpm active-servers
Protocol: TCP, Port: 50000

Protocol: UDP, Port: 50037
```

Meaning The output shows a list of the protocols and corresponding ports for which the device is configured as an RPM server.

Related Topics For a complete description of `show services rpm active-servers` output, see the *JUNOS System Basics and Services Command Reference*.

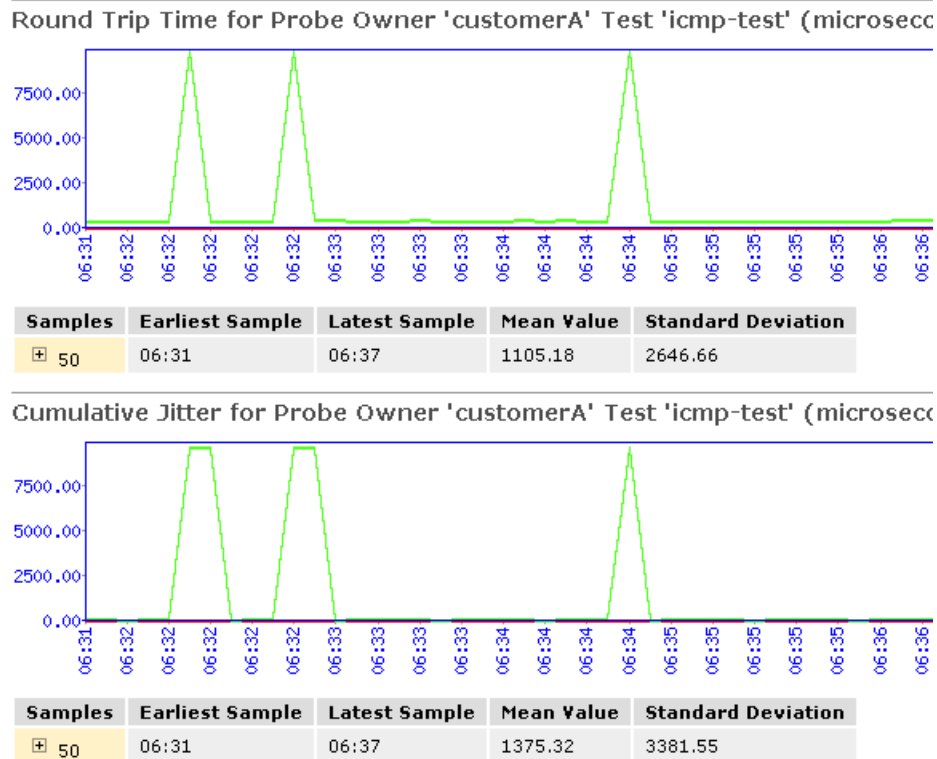
Monitoring RPM Probes

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 interface, or enter the following CLI show command:

```
show services rpm probe-results
```

In addition to the RPM statistics for each RPM test, the J-Web interface displays the round-trip times and cumulative jitter graphically. Figure 28 on page 418 shows sample graphs for an RPM test.

Figure 28: Sample RPM Graphs



In Figure 28 on page 418, 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 234 on page 419 summarizes key output fields in RPM displays.

Table 234: Summary of Key RPM Output Fields

Field	Values	Additional Information
Currently Running Tests		
Graph		Click the Graph 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.	
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: <ul style="list-style-type: none"> ■ http-get ■ http-get-metadata ■ icmp-ping ■ icmp-ping-timestamp ■ tcp-ping ■ udp-ping 	
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 J Series device to the remote server, as measured over the course of the test.	
Maximum RTT	Longest round-trip time from the J Series device to the remote server, as measured over the course of the test.	
Average RTT	Average round-trip time from the J Series device to the remote server, as measured over the course of the test.	
Standard Deviation RTT	Standard deviation of round-trip times from the J Series 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.	
Round-Trip Time for a Probe		
Samples	Total number of probes used for the data set.	The J Series 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.

Table 234: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
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 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 J Series 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.	
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The J Series 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.	

Part 6

Index

- Index on page 423

Index

Symbols

#, comments in configuration statements.....	xxv
#, configuration mode command prompt.....	30
(), in syntax descriptions.....	xxv
.gz.jc file extension <i>See</i> file encryption	
/cf/var/crash directory <i>See</i> crash files	
/cf/var/log directory <i>See</i> system logs	
/cf/var/tmp directory <i>See</i> temporary files	
/config directory	
file encryption <i>See</i> file encryption	
snapshots for boot directories (CLI).....	267
snapshots for boot directories (J-Web).....	266
/var/db/config directory <i>See</i> file encryption	
/var/db/scripts/commit directory <i>See</i> commit scripts	
/var/db/scripts/op directory <i>See</i> operation scripts	
/var/log directory <i>See</i> system log messages	
< >, in syntax descriptions.....	xxv
>, operational mode command prompt.....	29
? command	
for CLI online help.....	33
in configuration mode.....	30
in operational mode.....	29
[], in configuration statements.....	xxv
{ }, in configuration statements.....	xxv
(pipe) command.....	148
(pipe), in syntax descriptions.....	xxv

A

Access Manager license.....	314
access privileges	
denying and allowing commands.....	49
permission bits for.....	47
predefined.....	47
specifying (Quick Configuration).....	51
accounts <i>See</i> template accounts; user accounts	
action modifier	
packet-mode.....	292
activate system scripts commit command.....	138
activate system scripts op command.....	140
active routes, displaying.....	203
adaptive services interfaces	
alarm conditions and configuration options.....	242

addresses	
destination, displaying.....	203
administrator authentication	
support on J Series Services Routers.....	17
support on SRX100, SRX210 and SRX240	
devices.....	3
support on SRX3400 and SRX3600 devices.....	13
support on SRX5600 and SRX5800 devices.....	13
support on SRX650 devices.....	9
Advanced Encryption Standard (AES) <i>See</i> AES	
encryption	
AES encryption	
for Canada and U.S JUNOS.....	329
setting.....	330
agents, SNMP <i>See</i> SNMP agents	
alarm class <i>See</i> alarm severity	
ALARM LED, color.....	240
alarm severity	
configuring for an interface.....	245
major (red)	241
<i>See also</i> major alarms	
minor (yellow).....	241
<i>See also</i> minor alarms	
alarms	
active, displaying at login.....	246
conditions, on an interface.....	242
configurable.....	242
configuration requirements for interface	
alarms.....	245
licenses.....	244
major <i>See</i> major alarms	
minor <i>See</i> minor alarms	
overview.....	240
red <i>See</i> major alarms	
rescue configuration.....	244
severity <i>See</i> alarm severity	
support on J Series Services Routers.....	17
support on SRX100, SRX210 and SRX240	
devices.....	3
support on SRX3400 and SRX3600 devices.....	13
support on SRX650 devices.....	9
types.....	240
verifying.....	247
yellow <i>See</i> minor alarms	
alert logging severity.....	232
alias, CoS value.....	210

any level statement.....	236
any logging facility.....	232
archiving system logs.....	236
arithmetic operators, for multicast traffic.....	379
AS path, displaying.....	203
AT commands, for modem initialization	
description.....	69
modifying.....	79
attacks	
brute force, preventing.....	64
dictionary, preventing.....	64
authentication	
adding a RADIUS server (Quick Configuration).....	50
adding a TACACS+ server (Quick Configuration).....	50
local password, by default.....	51
login classes.....	47, 56
methods.....	46, 47
order of user authentication (configuration editor).....	55
RADIUS authentication (configuration editor).....	52
specifying a method (Quick Configuration).....	51
specifying access privileges (Quick Configuration).....	51
TACACS+ authentication (configuration editor).....	54
user accounts.....	46, 58
authorization logging facility.....	232
Autoinstallation	
support on SRX100, SRX210 and SRX240 devices.....	3
support on SRX650 devices.....	9
autoinstallation	
automatic configuration process.....	130
CLI configuration editor.....	131
default configuration file.....	130
establishing.....	127
host-specific configuration file.....	130
interfaces.....	128
IP address procurement process.....	129
J-Web configuration editor.....	131
overview.....	128
protocols for procuring an IP address.....	128
requirements.....	130
status.....	133
support on J Series Services Routers.....	17
TFTP server.....	129
verifying.....	133
autoinstallation, compatibility with the DHCP server.....	103
automatic configuration <i>See</i> autoinstallation	

B

basic connectivity	
secure Web access.....	37
BGP (Border Gateway Protocol)	
monitoring.....	206
peers, probes to <i>See</i> BGP RPM probes	
RPM probes to BGP neighbors <i>See</i> BGP RPM probes	
statistics.....	206
status.....	207
BGP groups, displaying.....	206
BGP neighbors	
directing RPM probes to.....	414
displaying.....	207
monitoring with RPM probes.....	412
BGP peers <i>See</i> BGP neighbors	
BGP route reflectors license.....	314
BGP routing information.....	206
BGP RPM probes	
directing to select BGP neighbors (configuration editor).....	414
overview.....	399
setting up on local and remote device (configuration editor).....	413
BGP sessions, status.....	207
binary operators, for multicast traffic.....	379
boot devices.....	263
configuring (CLI).....	266
configuring (J-Web).....	264
selecting (CLI).....	271, 272
selecting (J-Web).....	270
storing memory snapshots.....	268
<i>See also</i> CompactFlash card	
BOOTP, for autoinstallation.....	132
Border Gateway Protocol (BGP) route reflectors	
license.....	314
braces, in configuration statements.....	xxv
brackets	
angle, in syntax descriptions.....	xxv
square, in configuration statements.....	xxv
browser interface <i>See</i> J-Web interface	
brute force attacks, preventing.....	64
built-in Ethernet ports <i>See</i> Ethernet ports; management interfaces	
bypassing flow-based forwarding.....	289

C

caller ID, for dial-in over USB modems.....	74
<i>See also</i> dialer interface, for USB modem	
capturing packets <i>See</i> packet capture	
certificates <i>See</i> SSL certificates	
Challenge Handshake Authentication Protocol, enabling	
on dialer interfaces.....	75
change-log logging facility.....	232

- CHAP (Challenge Handshake Authentication Protocol),
 - enabling on dialer interfaces.....75
- chassis
 - monitoring.....153
 - power management.....154
- chassis management
 - support on SRX240 devices.....4
 - support on SRX3400 and SRX3600 devices.....13
 - support on SRX5600 and SRX5800 devices.....13
 - support on SRX650 devices.....9
- chassis software process.....229
- chassis-control
 - restart options.....273
- chassisd process.....229
- classifiers, CoS.....209
- Clean Up Files page.....324
- cleaning up files.....324, 328
- clear system services dhcp conflicts command.....104
- CLI *See* JUNOS CLI
- CLI configuration editor
 - autoinstallation.....131
 - CHAP on dialer interfaces.....75
 - controlling user access.....56
 - enabling commit scripts.....136
 - enabling operation scripts.....139
 - event policies.....141
 - interface alarms.....245
 - RADIUS authentication.....52
 - RPM.....406
 - secure access configuration.....42
 - SNMP.....93
 - statement types.....31
 - system log messages, sending to a file.....234
 - system log messages, sending to a terminal.....235
 - TACACS+ authentication.....54
 - USB modem connections.....71
- CLI terminal *See* JUNOS CLI
- code point aliases, CoS.....210
- command completion
 - description.....32
 - setting on and off.....35
- command hierarchy.....28
- command prompts
 - changing.....35
 - configuration mode (#).....30
 - operational mode (>).....29
- comments, in configuration statements.....xxv
- commit scripts
 - /var/db/scripts/commit directory.....136
 - disabling.....137
 - enabling.....136
 - overview.....135
 - superuser privileges required for.....136
- communities, SNMP *See* SNMP communities
- CompactFlash card
 - configuring.....267
 - configuring for failure snapshot storage.....268
 - corrupted.....251
- configuration
 - autoinstallation of.....127
 - consistency checking, with commit scripts.....135
 - downgrading software (CLI).....263
 - downgrading software (J-Web).....262
 - installation on multiple services routers.....127
 - modification and checking with operation
 - scripts.....138
 - rule enforcement, with commit scripts.....135
 - upgrading (CLI).....257
 - upgrading (J-Web).....255
- configuration files
 - decrypting.....323
 - encrypting.....323
- configuration management, automating.....135
 - See also* commit scripts; operation scripts
- configuration mode
 - commands.....30
 - prompt (#).....30
- Confirm File Delete page.....326
- console port
 - disabling.....62
 - securing.....61
- container statements.....31
- control plane logs.....233
- controlling user access.....56
- conventions
 - notice icons.....xxiv
 - text and syntax.....xxiv
- CoS (class of service)
 - classifiers.....209
 - CoS value aliases.....210
 - forwarding classes.....211
 - interfaces.....208
 - loss priority.....214
 - packet loss priority.....214
 - RED drop profiles.....210
 - rewrite rules.....212
 - RPM probe classification.....409
 - See also* TCP RPM probes; UDP RPM probes
 - scheduler maps.....213
- crash files
 - cleaning up (CLI).....328
 - cleaning up (J-Web).....324
 - downloading (J-Web).....325
- critical logging severity.....232
- cron logging facility.....232
- curly braces, in configuration statements.....xxv
- customer support.....xxvi
 - contacting JTAC.....xxvi

D

- daemon logging facility.....232
- daemons *See* processes, software
- Data Encryption Standard (DES) *See* DES encryption
- data plane logs.....233
- deactivate system scripts commit command.....137
- deactivate system scripts op command.....140
- debug logging severity.....233
- decryption, configuration files *See* file encryption
- default configuration file, for autoinstallation.....130
- delete system scripts commit command.....137
- delete system scripts op command.....140
- deleting
 - crash files (J-Web).....325
 - files, with caution.....326
 - licenses (CLI).....316
 - licenses (J-Web).....319
 - log files (J-Web).....325
 - temporary files (J-Web).....325
- DES encryption
 - for international JUNOS.....329
 - setting.....330
- destination address, displaying.....203
- device
 - automating operations and troubleshooting.....135
 - halting (CLI).....271
 - halting (J-Web).....269
 - packet capture.....381
 - rebooting (J-Web).....269
- DHCP (Dynamic Host Configuration Protocol)
 - autoinstallation, compatibility with.....103
 - conflict detection and resolution.....104
 - interface restrictions.....104
 - options.....103
 - overview.....102
 - See also* DHCP leases; DHCP pages; DHCP pools; DHCP server
 - server function.....101
 - support on J Series Services Routers.....18
 - support on SRX100, SRX210 and SRX240
 - devices.....4
 - support on SRX3400 and SRX3600 devices.....14
 - support on SRX5600 and SRX5800 devices.....14
 - support on SRX650 devices.....10
 - verification.....122
- DHCP server
 - preparation.....104
 - sample configuration.....116
 - subnet and single client.....117
 - verifying operation.....125
- dhcpcd process.....229
- diagnosis
 - alarm configurations.....247
 - automating with event policies.....140
 - See also* event policies
 - CLI command summary.....337
 - displaying firewall filter for.....392
 - displaying packet capture configurations.....391
 - displaying selective stateless packet-based services
 - configuration.....298, 307
 - interfaces.....242, 373
 - J-Web tools overview.....336
 - license infringement.....244
 - monitoring network performance.....395
 - MPLS connections (J-Web).....345
 - multicast paths.....369
 - network traffic.....375
 - packet capture.....381
 - packet capture (J-Web).....354
 - ping command.....359
 - ping host (J-Web).....342
 - ping MPLS (J-Web).....345
 - ports.....242
 - preparation.....341
 - SNMP health monitor.....87
 - system logs.....229
 - system operation.....373
 - traceroute (J-Web).....350
 - traceroute command.....365
 - traceroute monitor command.....365
 - traffic analysis with packet capture.....381
 - verifying captured packets.....392
 - verifying DHCP server operation.....125
 - verifying dialer interfaces.....82
 - verifying RPM probe servers.....417
 - verifying RPM statistics.....416
 - verifying USB modem interfaces.....81
- diagnostic commands.....337
- diagnostic tools
 - support on J Series Services Routers.....18
 - support on SRX100, SRX210 and SRX240
 - devices.....4
 - support on SRX3400 and SRX3600 devices.....14
 - support on SRX5600 and SRX5800 devices.....14
 - support on SRX650 devices.....10
- dial-in, USB modem (configuration editor).....74
 - See also* dialer interface, for USB modem
- dial-up modem connection
 - configuring device end.....71
 - configuring user end.....77
 - connecting device end.....71
 - connecting user end.....78
- dialer interface, for USB modem
 - adding (configuration editor).....73
 - See also* USB modem connections
 - CHAP for PPP (configuration editor).....75
 - dial-in (configuration editor).....74
 - limitations.....68
 - naming convention.....68
 - restrictions.....68
 - verifying.....82

dialer pools, for USB modems72
See also dialer interface, for USB modem

dictionary attacks, preventing.....64

DiffServ code points, bits for RPM probes.....403

disabling

- commit scripts.....137
- console port.....62
- operation scripts.....140
- packet capture.....389
- root login to console port.....62
- system logs.....236

disconnection of console cable for console logout.....62

dl0.....68

documentation set

- comments on.....xxvi

downgrading

- software, with J-Web.....262
- software, with the CLI263

download URL.....254

downloading

- configuration, with autoinstallation.....130
- crash files (J-Web).....325
- licenses (J-Web).....319
- log files (J-Web).....325
- software upgrades.....254
- temporary files (J-Web).....325

drop probabilities, CoS.....210

drop profiles, CoS.....210

DS1 ports *See* T1 ports

DS3 ports *See* E3 ports; T3 ports

DSCPs (DiffServ code points), bits for RPM

- probes.....403

dynamic host configuration process.....229

Dynamic Host Configuration Protocol *See* DHCP

E

E3 ports, alarm conditions and configuration

- options.....243

egress *See* RPM probes, outbound times

emergency logging severity.....232

encapsulation, modifying on packet capture-enabled

- interfaces.....390

encrypted access

- through HTTPS.....37
- through SSL.....37

encryption, configuration files *See* file encryption

enforcement of configuration rules.....135

environment, CLI

- displaying.....34
- setting.....34

error logging severity.....232

Ethernet ports

- alarm conditions and configuration options.....242
- autoinstallation on.....128

- configuring alarms on.....245
- Gigabit Ethernet ports, SNMP support.....85

event notifications, automating response to with event

- policies.....140
- See also* SNMP traps; system log messages

event policies

- configuration editor.....141
- overview.....141
- support on J Series Services Routers.....18
- support on SRX100, SRX210 and SRX240
- devices.....5
- support on SRX3400 and SRX3600 devices.....14
- support on SRX5600 and SRX5800 devices.....14
- support on SRX650 devices.....10

event viewer, J-Web

- overview.....236
- See also* system log messages

Extensible Stylesheet Language Transformations (XSLT)

- See* commit scripts; operation scripts

F

facility none statement.....236

feature licenses *See* licenses

file encryption

- .gz.jc file extension.....329
- decrypting configuration files.....331
- directories.....329
- encrypting configuration files.....330
- encryption algorithms required for JUNOS
- versions.....329
- encryption key.....329
- overview.....329
- superuser privileges required for.....329

file management

- configuration files.....323
- crash files (CLI).....328
- crash files (J-Web).....324
- encryption-decryption *See* file encryption
- log files.....323
- log files (CLI).....328
- log files (J-Web).....324
- packet capture file creation.....384
- support on J Series Services Routers.....18
- support on SRX100, SRX210 and SRX240
- devices.....4
- support on SRX3400 and SRX3600 devices.....14
- support on SRX5600 and SRX5800 devices.....14
- support on SRX650 devices.....10
- temporary files (CLI).....328
- temporary files (J-Web).....324

filtering

- command output.....148

firewall authentication process.....229

firewall filters	
for packet capture, configuring.....	388
for packet capture, overview.....	384
flowd process.....	229
font conventions.....	xxiv
forwarding classes, CoS.....	211
forwarding software process.....	229
frequency, test <i>See</i> RPM probes, test intervals	
fwauthd process.....	229

G

get requests.....	86
glossary	
alarms.....	239
autoinstallation.....	127
DHCP.....	101
diagnostic.....	335
monitoring.....	148
packet capture.....	381
RPM.....	395
secure Web access.....	37
system logs.....	229
USB modems.....	67
user authentication.....	45
group licenses.....	318
groups	
BGP, displaying.....	206
for SNMP traps.....	95

H

halting a device	
with J-Web.....	269
with the CLI.....	271
halting a device immediately	
with J-Web.....	270
with the CLI.....	272
hardware	
major (red) alarm conditions on.....	241
supported platforms.....	xxii
timestamp <i>See</i> RPM probe timestamps	
Hayes-compatible modem commands, USB modem	
initialization.....	79
health monitor <i>See</i> SNMP health monitor	
heat status, checking.....	154
help apropos command.....	33
help reference command.....	33
help syslog ? command.....	141
help topic command.....	33
Help, JUNOS CLI.....	33
host reachability	
ping command.....	359
ping host (J-Web).....	342
host-specific configuration file, for	
autoinstallation.....	130

hostname	
monitoring traffic by matching.....	377
opening an SSH session to.....	63
overriding for SNMP (configuration editor).....	94
overriding for SNMP (Quick Configuration).....	90
pinging (CLI).....	359
pinging (J-Web).....	343
resolving.....	116
SNMP trap target (Quick Configuration).....	91
telnetting to.....	63
tracing a route to (CLI).....	366, 367
tracing a route to (J-Web).....	352
hostname.conf file, for autoinstallation.....	130
HTTP (Hypertext Transfer Protocol)	
enabling Web access (configuration editor).....	42
enabling Web access (Quick Configuration).....	39
on built-in management interfaces.....	38
support on J Series Services Routers.....	19
support on SRX210 and SRX240 devices.....	5
support on SRX3400 and SRX3600 devices.....	14
support on SRX5600 and SRX5800 devices.....	14
support on SRX650 devices.....	11
verifying configuration.....	43
HTTP (Hypertext Transfer Protocol), RPM probes.....	396
HTTPS (Hypertext Transfer Protocol over SSL)	
enabling secure access (configuration editor).....	42
enabling secure access (Quick Configuration).....	39
Quick Configuration.....	39
recommended for secure access.....	38
verifying secure access configuration.....	43
HTTPS Web access, establishing.....	37
Hypertext Transfer Protocol <i>See</i> HTTP	
Hypertext Transfer Protocol over SSL <i>See</i> HTTPS	
Hypertext Transfer Protocol, RPM probes.....	396

I

ICMP (Internet Control Message Protocol)	
RPM probes, description.....	396
RPM probes, inbound and outbound times.....	398
RPM probes, setting.....	406
idle time, setting for a CLI session.....	35
IDP signature update license.....	314
ifd process.....	229
iked process.....	229
inbound time <i>See</i> RPM probes	
info logging severity.....	233
ingress <i>See</i> RPM probes, inbound times	
init-command-string command.....	69
Install Remote page.....	255
field summary.....	256, 265
installation	
licenses (CLI).....	315
licenses (J-Web).....	318
software upgrades (CLI).....	257

software upgrades, from a remote server.....	255
software upgrades, uploading.....	256
Instance to which this connection belongs	
description.....	340
using.....	348
interactive-commands logging facility.....	232
interface software process.....	229
interfaces <i>See</i> management interfaces; network	
interfaces; ports	
internal CompactFlash card <i>See</i> CompactFlash card	
Internet Explorer, modifying for worldwide version of	
JUNOS Software.....	25
Internet Key Exchange process.....	229
intervals, probe and test <i>See</i> RPM probes	
Intrusion Detection and Prevention (IDP) signature	
update license.....	314
ipconfig command.....	125
explanation.....	126

J

J Series.....	323
alarms.....	239
automating operations with scripts.....	135
automating troubleshooting with scripts and event	
policies.....	135
licenses.....	313
managing user authentication.....	45
monitoring	147
network management.....	85
packet capture.....	381
performance monitoring.....	395
system log messages.....	229
user interfaces <i>See</i> user interfaces	
J Series devices	
supported features.....	17
J Series Services Router	
licenses.....	314
J-Web configuration editor	
autoinstallation.....	131
CHAP on dialer interfaces.....	75
controlling user access.....	56
enabling commit scripts.....	136
enabling operation scripts.....	139
event policies.....	141
interface alarms.....	245
RADIUS authentication.....	52
RPM.....	406
secure access.....	42
SNMP.....	93
system log messages, sending to a file.....	234
system log messages, sending to a terminal.....	235
TACACS+ authentication.....	54
USB modem connections.....	71
J-Web interface	
context-sensitive help.....	33
Diagnose options.....	336
event viewer.....	236
Internet Explorer, modifying for worldwide version	
of JUNOS Software.....	25
managing files.....	323
managing licenses.....	317
overview.....	24
page layout.....	26
sessions.....	27
starting.....	25
windows, multiple, unpredictable results	
with.....	27
jitter	
description.....	398
<i>See also</i> RPM probes	
in RPM probes, improving with timestamps.....	397
monitoring.....	420
threshold, setting.....	403
Juniper-Kaspersky Anti-Virus license.....	314
Juniper-Symantec Anti-Spam license.....	314
Juniper-WebSense Integrated Web Filtering	
license.....	314
JUNOS CLI	
access privilege levels.....	48
automatic command execution with event	
policies.....	141
CLI terminal.....	29
command completion.....	32
command hierarchy.....	28
command modes.....	25
command prompts <i>See</i> command prompts	
console.....	29
context-sensitive help.....	33
denying and allowing commands.....	49
diagnostic command summary.....	338
editing keystrokes.....	31
environment, changing.....	34
filtering command output.....	148
idle time.....	35
managing licenses.....	315
overview.....	25
screen length.....	35
screen width.....	35
ssh.....	29
starting.....	29
support on J Series Services Routers.....	18
support on SRX100, SRX210 and SRX240	
devices.....	4
support on SRX3400 and SRX3600 devices.....	14
support on SRX5600 and SRX5800 devices.....	14
support on SRX650 devices.....	10
telnet.....	29
terminal type.....	36
working directory.....	35

- JUNOS Software
 - autoinstallation.....127
 - encryption *See* file encryption
 - Internet Explorer, modifying for worldwide version.....25
 - known problems, operation scripts as workarounds.....138
 - processes.....229
 - upgrading.....251
 - USB modems for remote management.....67
 - worldwide version, modifying Internet Explorer for.....25
 - junos-jseries package *See* upgrades
 - JUNOScope application.....23
 - JUNOScript API
 - enabling secure access.....39
 - verifying secure access configuration.....43
 - JUNOScript Extensible Markup Language (XML) *See* commit scripts; operation scripts
 - JUNOScript over SSL.....39
- K**
- kernel logging facility.....232
 - key sequences, editing, in CLI.....31
- L**
- label-switched paths *See* LSPs
 - latency, in RPM probes, improving with timestamps.....397
 - Layer 2 circuits, monitoring.....345
 - Layer 2 VPNs, monitoring.....345
 - Layer 3 VPNs, monitoring.....345
 - leaf statements.....31
 - libpcap format, for packet capture files.....393
 - license infringement
 - identifying any licenses needed.....318
 - verifying license usage.....320
 - verifying licenses installed.....320
 - license keys
 - components.....314
 - displaying (CLI).....321
 - displaying (J-Web).....319
 - status.....318
 - version.....318
 - licenses
 - Access Manager.....314
 - adding (CLI).....315
 - adding (J-Web).....318
 - BGP route reflectors.....314
 - deleting (CLI).....316
 - deleting (J-Web).....319
 - displaying (CLI).....320
 - displaying (J-Web).....317
 - displaying usage.....320
 - downloading (J-Web).....319
 - group.....318
 - IDP signature update.....314
 - infringement, preventing.....317
 - See also* license infringement
 - J Series Services Router314
 - Juniper-Kaspersky Anti-Virus.....314
 - Juniper-Symantec Anti-Spam.....314
 - Juniper-WebSense Integrated Web Filtering
 - license.....314
 - key.....314
 - See also* license keys
 - managing (CLI).....315
 - managing (J-Web).....317
 - overview.....313
 - saving (CLI).....317
 - SRX Series Services Gateway.....314
 - SRX100 Memory Upgrade license.....314
 - updating (CLI).....316
 - UTM.....314
 - verifying.....319
 - licenses, alarm conditions and remedies.....244
 - limitations
 - ALARM LED lights yellow whether alarm is minor
 - or major.....240
 - DHCP, no support on VPN interfaces.....104
 - MPLS, no LSP statistics on outbound device.....216
 - mtrace from-source packet statistics always
 - 0.....371
 - performance degradation with monitor traffic
 - command.....375
 - PPP, no J-Web monitoring information
 - available.....222
 - Server relay and DHCP client cannot coexist in device.....102
 - SNMP not supported on Gigabit Ethernet
 - interfaces.....85
 - software downgrade cannot be undone.....263
 - local password
 - default authentication method for system.....51
 - method for user authentication (Quick Configuration).....51
 - order of user authentication (configuration editor).....56
 - overview.....46, 47
 - local template accounts.....60
 - Locate LSP from interface name
 - description.....340
 - using.....348
 - Locate LSP from virtual circuit information
 - description.....340
 - using.....349
 - Locate LSP using interface name
 - description.....340
 - using.....348

log files
 archiving.....323
 deleting unused files.....323
 rotating.....323
 support on J Series Services Routers.....19
 support on SRX100, SRX210 and SRX240 devices.....6
 Log Files page (Download).....325
 log messages *See* system log messages
 logging facilities.....232
 logging severity levels.....232
 logical interfaces, CoS.....208
 logical operators, for multicast traffic.....378
 login classes
 defining (configuration editor).....57
 permission bits for.....48
 predefined permissions.....47
 specifying (Quick Configuration).....51
 login retry limits, setting.....64
 logs *See* system logs
 loss priority, CoS.....214
 LSPs (label-switched paths)
 information about.....216
 monitoring, with ping MPLS.....345
 statistics.....217

M

major (red) alarms
 description.....241
 management device
 diagnosing problems from.....336
 monitoring from.....148
 Management Information Bases *See* MIBs
 management interfaces
 alarm conditions and configuration options.....242
 configuring alarms on.....245
 monitoring.....149, 373
 statistics.....373
 management software process.....229
 managing
 files.....323
 reboots.....269
 snapshots.....263
 software.....251
 user authentication.....45
 manuals
 comments on.....xxvi
 match conditions, for multicast traffic
 377
 memory usage
 monitoring, SNMP *See* SNMP health monitor
 messages *See* system log messages
 mgd process.....229

MIBs (Management Information Bases)
 controlling access (configuration editor).....96
 enterprise.....86
 standard.....86
 system identification (configuration editor).....93
 URLs for download.....86
 views (configuration editor).....96
 Microsoft Windows XP commands, connecting to
 device from a management device.....77
 minor (yellow) alarms
 description.....241
 modem connection to device USB port *See* USB modem connections
 modem connection to user management device *See* USB modem connections
 monitor interface command.....373
 controlling output.....374
 monitor interface traffic command.....373
 controlling output.....374
 monitor list command.....373
 monitor start command.....373
 monitor stop command.....373
 monitor traffic command.....375
 options.....375
 performance impact.....375
 monitor traffic matching command.....377
 arithmetic, binary, and relational operators.....379
 logical operators.....378
 match conditions.....377
 monitoring
 BGP.....206
 BGP neighbors, with RPM probes.....412
 chassis.....153
 device health *See* SNMP health monitor
 health of the device *See* SNMP health monitor
 interfaces.....149, 373
 Layer 2 circuits.....345
 Layer 2 VPNs.....345
 Layer 3 VPNs.....345
 MPLS traffic
 engineering.....214, 215, 216, 217, 218
 multicast paths.....369
 network interface traffic.....375
 network traffic with packet capture.....381
 OSPF.....205
 ports.....149
 PPP (CLI).....222
 PPPoE.....219
 preparation.....341
 RIP.....204
 routing information.....202
 routing tables.....202
 RPM probes.....418
 SNMP health monitor *See* SNMP health monitor
 system log messages.....229

system logs.....	373
trace files.....	373
monitoring the wx interface.....	223
MPLS (Multiprotocol Label Switching)	
connections, checking.....	345
LSPs.....	216
monitoring interfaces.....	215
monitoring LSP information.....	215
monitoring LSP statistics.....	216, 217
monitoring MPLS interfaces.....	215
monitoring RSVP interfaces.....	218
monitoring RSVP sessions.....	217, 218
monitoring traffic engineering.....	214
mtrace monitor command.....	372
results.....	372
mtrace-from-source command.....	370
options.....	370
results.....	371
multicast	
trace operations, displaying.....	372
tracing paths.....	370
MultiModem, recommended for USB modem	
connections.....	67
multiple devices, using snapshots to replicate	
configurations	
CLI.....	267
J-Web.....	265
multiple routers	
deploying <i>See</i> autoinstallation	
Multiprotocol Label Switching <i>See</i> MPLS	
N	
neighbors, BGP <i>See</i> BGP neighbors; BGP RPM probes	
network interfaces	
alarm conditions and configuration options.....	242
configuring alarms on.....	245
integrated services, alarm conditions and	
configuration options.....	242
monitoring.....	149, 373
monitoring MPLS traffic engineering.....	215
monitoring traffic.....	375
monitoring, CoS.....	208
monitoring, PPPoE.....	220
monitoring, RSVP.....	219
packet capture, configuring on.....	387
packet capture, disabling before changing	
encapsulation.....	390
packet capture, supported on.....	383
services, alarm conditions and configuration	
options.....	243
statistics.....	373
network management.....	85
automating with operation scripts.....	138
diagnosis and problem-solving with scripts.....	138
<i>See also</i> SNMP	
network management system (NMS).....	87
network performance <i>See</i> RPM	
network security process.....	229
network.conf file, default for	
autoinstallation.....	130, 131
next hop, displaying.....	203
NMS (network management system).....	87
no-world-readable statement.....	236
notice icons.....	xxiv
notice logging severity.....	233
notifications <i>See</i> event policies; system log messages;	
SNMP traps	
nsd process.....	229
nsrpd process.....	229
O	
object identifiers (OIDs).....	86
OIDs (object identifiers).....	86
op command.....	139
Open Shortest Path First <i>See</i> OSPF	
openssl command.....	39
operation scripts	
/var/db/scripts/op directory.....	139
disabling.....	140
enabling.....	139
executing from the CLI.....	139
executing within an event policy.....	140
overview.....	138
superuser privileges required for.....	139
support on J Series Services Routers.....	18
support on SRX100, SRX210 and SRX240	
devices.....	5
support on SRX3400 and SRX3600 devices.....	14
support on SRX5600 and SRX5800 devices.....	14
support on SRX650 devices.....	10
operational mode	
commands.....	29
prompt (>).....	29
operational mode, filtering command output.....	148
operator login class permissions.....	47
operators	
arithmetic, binary, and relational operators.....	379
logical.....	378
OSPF (Open Shortest Path First)	
monitoring.....	204
statistics.....	205
OSPF interfaces	
displaying.....	205
status.....	205
OSPF neighbors	
displaying.....	205
status.....	205
OSPF routing information.....	204
outbound time <i>See</i> RPM probes	

P

- packet capture
 - configuring.....387
 - configuring (J-Web).....354
 - configuring on an interface.....387
 - device interfaces supported.....383
 - disabling.....389
 - disabling before changing encapsulation on
 - interfaces.....390
 - displaying configurations.....391
 - displaying firewall filter for.....392
 - enabling.....385
 - encapsulation on interfaces, disabling before
 - modifying.....390
 - files *See* packet capture files
 - firewall filters, configuring.....388
 - firewall filters, overview.....384
 - J-Web tool.....354
 - overview.....382
 - overview (J-Web).....354
 - preparation.....385
 - support on J Series Services Routers.....19
 - verifying captured packets.....392
 - verifying configuration.....391
 - verifying firewall filter for.....392
- packet capture files
 - analyzing.....384
 - libpcap format.....393
 - overview.....384
 - renaming before modifying encapsulation on
 - interfaces.....390
- packet capture options
 - support on SRX100, SRX210 and SRX240
 - devices.....5
- Packet Capture page
 - field summary.....355
 - results.....358
- packet loss priority, CoS.....214
- packet-based forwarding
 - selective stateless.....289
- packet-mode.....292
- packets
 - capturing.....381
 - capturing with J-Web packet capture.....354
 - monitoring jitter.....420
 - monitoring packet loss.....419
 - monitoring round-trip times.....419
 - multicast, tracking370
 - packet capture.....381
 - packet capture (J-Web).....354
 - tracking MPLS.....350
 - tracking with J-Web traceroute.....350
 - tracking with the traceroute command.....365
- parentheses, in syntax descriptions.....xxv
- partitioning a boot medium.....267
- password retry limits, setting.....65
- passwords
 - for downloading software upgrades.....254
 - local password method for user authentication
 - (Quick Configuration).....51
 - See also* local password
 - retry limits.....64
 - setting login retry limits.....64
- paths, multicast, tracing.....369
- PCAP *See* packet capture
- peers, BGP *See* BGP neighbors; BGP RPM probes
- performance, monitoring *See* RPM
- permission bits, for login classes.....48
- permissions
 - denying and allowing commands.....49
 - predefined.....47
- physical interfaces, CoS.....208
- PIMs (Physical Interface Modules)
 - checking power and heat status.....154
- ping
 - host reachability (CLI).....359
 - host reachability (J-Web).....342
 - ICMP probes.....406
 - indications.....345
 - RPM probes *See* RPM probes
 - TCP and UDP probes.....409
- ping command.....359
 - DHCP server operation.....125
 - DHCP server operation, explanation.....125
 - options.....359
- Ping end point of LSP
 - description.....340
 - using.....349
- ping host
 - results.....345
 - support on J Series Services Routers.....18
 - support on SRX100, SRX210 and SRX240
 - devices.....4
 - support on SRX3400 and SRX3600 devices.....14
 - support on SRX5600 and SRX5800 devices.....14
 - support on SRX650 devices.....10
- Ping Host page.....343
 - field summary.....343
 - results.....344
- Ping LDP-signaled LSP
 - description.....340
 - using.....347
- Ping LSP to Layer 3 VPN prefix
 - description.....340
 - using.....348
- ping MPLS (J-Web)
 - indications.....350
 - Layer 2 circuits.....345
 - Layer 2 VPNs.....345
 - Layer 3 VPNs.....345
 - LSP state.....345
 - options.....339

requirements.....	341
results.....	350
ping mpls l2circuit command.....	365
results.....	350
ping mpls l2vpn command.....	363
results.....	350
ping mpls l3vpn command.....	363
results.....	350
ping mpls ldp command.....	362
results.....	350
ping mpls lsp-end-point command.....	362
results.....	350
Ping MPLS page.....	347
field summary.....	347
results.....	350
ping mpls rsvp command.....	362
results.....	350
Ping RSVP-signaled LSP	
description.....	339
using.....	347
pipe () command, to filter output.....	148
Point-to-Point Protocol <i>See</i> PPP	
Point-to-Point Protocol over Ethernet <i>See</i> PPPoE	
ports	
alarm conditions and configuration options.....	242
configuring alarms on.....	245
console port, securing.....	61
DHCP interface restrictions.....	104
individual port types.....	242
monitoring.....	149
power management, chassis.....	154
PPP (Point-to-Point Protocol)	
CHAP on dialer interfaces.....	75
monitoring (CLI).....	222
PPPoE (Point-to-Point Protocol over Ethernet)	
interfaces.....	220
monitoring.....	219
session status.....	220
statistics.....	220
version information.....	221
printf statements.....	138
probe loss	
monitoring.....	419
threshold, setting.....	403
probes, monitoring.....	219, 418
<i>See also</i> RPM probes	
processes, software	
chassis process.....	229
forwarding process.....	229
interface process.....	229
management process.....	229
routing protocol process.....	229
prompt <i>See</i> command prompts; restart-after-upgrade prompt	

protocols	
DHCP <i>See</i> DHCP	
originating, displaying.....	203
OSPF, monitoring.....	204
PPP, monitoring.....	222
RIP, monitoring.....	204
routing protocols, monitoring.....	202, 206

Q

Quick Configuration	
adding users.....	51
authentication method.....	51
Packet Capture page.....	355
Packet Capture results page.....	358
RADIUS server.....	50
RPM pages.....	400, 401
secure Web access.....	39
SNMP page.....	89
TACACS+ server.....	50
user management.....	50

R

RADIUS	
adding a server (Quick Configuration).....	50
authentication (configuration editor).....	52
order of user authentication (configuration editor).....	56
secret (configuration editor).....	53
specifying for authentication (Quick Configuration).....	51
random early detection (RED) drop profiles, CoS.....	210
RARP, for autoinstallation.....	132
read-only login class permissions.....	47
real-time performance monitoring <i>See</i> RPM	
reboot immediately	
with J-Web.....	270
with the CLI.....	271
rebooting	
with J-Web	269
with the CLI.....	271
RED drop profiles, CoS.....	210
registration form, for software upgrades.....	252, 253
relational operators, for multicast traffic.....	379
remote accounts	
accessing with SSH (CLI).....	63
accessing with Telnet (CLI).....	62
remote template accounts.....	59
remote connection to device	
connecting USB modem to device.....	71
<i>See also</i> USB modem connections	
connecting USB modem to user management device.....	77
<i>See also</i> USB modem connections	

- remote management, with USB modems.....67
 - See also* USB modem connections; USB modems
- remote monitoring (RMON) *See* SNMP health monitor
- remote server, upgrading from.....255
- remote template accounts.....59
- request interface modem reset umd0 command.....80
- request system halt command.....271
 - options.....272
- request system license add command.....315
- request system license add terminal command.....316
- request system license delete command.....316
- request system license save command.....317
- request system license update command.....316
- request system reboot command.....271
 - options.....271
- request system set-encryption-key algorithm des
 - command.....330
- request system set-encryption-key command.....330
- request system set-encryption-key des unique.....330
- request system set-encryption-key unique.....330
- request system snapshot command.....266
 - options.....267
- request system software add validate unlink reboot
 - command.....258
- request system storage cleanup command.....328
- request system storage cleanup dry-run
 - command.....328
- rescue configuration, alarm about.....244
- Resource Reservation Protocol *See* RSVP
- restart-after-upgrade prompt.....35
- retry limits for passwords.....64
- Reverse Address Resolution Protocol (RARP), for
 - autoinstallation.....132
- reverse SSH.....66
- Reverse telnet
 - support on J Series Services Routers.....17
- reverse Telnet.....65
- reverting to a previous configuration file (J-Web).....262
- rewrite rules, CoS.....212
- RIP (Routing Information Protocol)
 - monitoring.....204
 - statistics.....204
- RIP neighbors
 - displaying.....204
 - status.....204
- RIP routing information.....204
- RMON (remote monitoring) *See* SNMP health monitor
- rolling back a configuration file, to downgrade software
 - (CLI).....263
- root login to the console, disabling.....62
- rotating files.....325
- round-trip time
 - description.....398
 - See also* RPM probes
 - threshold, setting.....403
- route reflectors, BGP, license.....314
- router context
 - support on J Series Services Routers.....19
- router.conf file, for autoinstallation.....130
- routing
 - monitoring.....202
 - traceroute (J-Web).....350
 - traceroute command.....365
 - traceroute monitor command.....365
- routing policies
 - export, displaying.....207
 - import, displaying.....207
- routing protocol software process.....229
- routing table
 - displaying.....203
 - monitoring.....202
- rpdp process.....229
- RPM (real-time performance monitoring)
 - basic probes (configuration editor).....406
 - BGP monitoring *See* BGP RPM probes
 - inbound and outbound times.....398
 - jitter, viewing.....420
 - monitoring probes.....418
 - overview.....396
 - See also* RPM probes
 - preparation.....399
 - probe and test intervals.....397
 - probe counts.....399
 - Quick Configuration.....400
 - round-trip times, description.....398
 - round-trip times, viewing.....419
 - sample configuration.....415
 - sample graphs.....418
 - statistics.....398
 - statistics, verifying.....416
 - TCP probes (configuration editor).....409
 - See also* TCP RPM probes
 - tests.....397
 - tests, viewing.....419
 - threshold values.....399
 - tuning probes.....411
 - UDP probes (configuration editor).....409
 - See also* UDP RPM probes
 - verifying probe servers.....417
- RPM pages.....400, 401
 - field summary.....402
- RPM probe options
 - support on SRX100, SRX210 and SRX240
 - devices.....5
 - support on SRX650 device.....11
- RPM probe timestamps
 - overview.....397
 - setting (configuration editor).....406
- RPM probes
 - basic (configuration editor).....406
 - BGP neighbors *See* BGP RPM probes
 - cumulative jitter.....420

current tests.....	419	RPM probes.....	415
DSCP bits (Quick Configuration).....	403	RPM test graphs.....	418
graph results.....	418	TCP and UDP probes.....	409
ICMP (configuration editor).....	406	user account.....	58
inbound times.....	398	saving licenses (CLI).....	317
jitter threshold.....	403	scheduler maps, CoS.....	213
monitoring.....	418	scheduling a reboot	
outbound times.....	398	with J-Web.....	270
probe count, setting (Quick Configuration).....	402	with the CLI.....	271
probe count, tuning.....	412	screen length, CLI, setting	35
probe counts.....	399	screen width, CLI, setting	35
probe intervals.....	397	scripts <i>See</i> commit scripts; operation scripts	
probe intervals, setting (Quick Configuration).....	402	secret	
probe intervals, tuning.....	412	RADIUS (configuration editor).....	53
probe loss count.....	403	TACACS+ (configuration editor).....	55
probe owner.....	402	secure access	
probe type, setting (Quick Configuration).....	402	establishing.....	37
probe types.....	396	generating SSL certificates.....	39
round-trip time threshold.....	403	HTTPS access (configuration editor).....	42
round-trip times, description.....	398	HTTPS access (Quick Configuration).....	39
round-trip times, viewing.....	419	HTTPS recommended.....	38
SNMP traps (Quick Configuration).....	404	installing SSL certificates (configuration editor).....	42
source address, setting.....	412	installing SSL certificates (Quick Configuration).....	39
support on J Series Services Routers.....	19	JUNOScript SSL access.....	39
TCP (configuration editor).....	409	overview.....	38
<i>See also</i> TCP RPM probes		requirements.....	38
TCP server port.....	405	sample configuration.....	43
test intervals.....	397	support on J Series Services Routers.....	19
test intervals, setting (Quick Configuration).....	402	support on SRX100, SRX210 and SRX240 devices.....	5
test target.....	402	support on SRX3400 and SRX3600 devices.....	14
threshold values, description.....	399	support on SRX5600 and SRX5800 devices.....	14
threshold values, setting (Quick Configuration).....	403	support on SRX650 devices.....	11
timestamps <i>See</i> RPM probe timestamps		verifying secure access configuration.....	43
tuning.....	411	secure context	
UDP (configuration editor).....	409	support on J Series Services Routers.....	19
<i>See also</i> UDP RPM probes		support on SRX100, SRX210 and SRX240 devices.....	5
UDP server port.....	405	support on SRX650 devices.....	11
verifying TCP and UDP probe servers.....	417	Secure Sockets Layer <i>See</i> SSL	
RSVP (Resource Reservation Protocol)		security	
interfaces, monitoring.....	219	access privileges.....	47, 56
sessions, monitoring.....	218	configuration file encryption.....	329
RTT <i>See</i> RPM probes, round-trip times		<i>See also</i> file encryption	
		console port security.....	61
S		packet capture for intrusion detection.....	382
sample configuration		password retry limits.....	64
for secure access.....	43	user accounts.....	46, 58
for SSL certificates.....	43	user authentication.....	46
sample configurations		selective stateless packet-based services.....	289
firewall filter configurations.....	299, 307	configuring.....	292
samples		end-to-end packet-based example.....	294
alarm configuration.....	247	limitations.....	292
basic RPM probes.....	406	overview.....	291
local template account.....	60		

- packet-based to flow-based example.....303
 - verifying configuration.....298, 307
- serial cable, disconnection for console logout.....62
- Serial Line Address Resolution Protocol (SLARP), for
 - autoinstallation.....132
- serial ports
 - alarm conditions and configuration options.....242
 - autoinstallation on.....128
 - configuring alarms on.....245
- Series
 - user interfaces *See* user interfaces
- Services Gateway
 - licenses.....313
 - user interfaces *See* user interfaces
- services module
 - alarm conditions and configuration options.....243
- Services Router
 - as a DHCP server.....101
 - diagnosis.....335
 - licenses.....313
 - monitoring147
 - network management.....85
 - performance monitoring.....395
 - user interfaces *See* user interfaces
- services router
 - autoinstallation.....127
 - bring components online/offline.....272
 - multiple, deploying *See* autoinstallation
 - rebooting (CLI).....271
 - software upgrades.....251
 - USB modems for remote management.....67
- sessions
 - BGP peer, status details.....207
 - BGP peer, status summary.....207
 - RSVP, monitoring.....218
 - Telnet.....63
- sessions, J-Web.....27
- set cli commands.....34
- set no-encrypt-configuration-files command.....331
- set requests.....86
- set system dump-device command.....268
 - options.....268
- severity levels
 - for alarms *See* alarm severity
 - for system logs.....232
- show bgp neighbor command.....206
- show bgp summary command.....206
- show chassis alarms command.....247, 248
- show chassis environment command.....153
- show chassis hardware command.....151, 152, 153
- show chassis power-ratings command.....154
- show chassis redundant-power-supply command.....154
- show chassis routing-engine command.....153, 156
- show class-of-service classifier command.....209
- show class-of-service code-point-aliases
 - command.....210
- show class-of-service command.....208
- show class-of-service drop-profile command.....210
- show class-of-service forwarding-class command.....211
- show class-of-service rewrite-rules command.....212
- show class-of-service scheduler-map command.....213
- show cli command.....34
- show firewall command.....298, 307
- show firewall filter dest-all command.....392
- show interfaces detail command.....149
- show interfaces dl0 extensive command.....82
- show interfaces interface-name command.....149
- show interfaces pp0 command.....220
- show interfaces terse command.....149
- show interfaces umd0 extensive command.....81
 - explanation, for USB modem interfaces.....81
- show log command.....231
- show mpls interface command.....215
- show mpls lsp command.....215
- show mpls statistics command.....216
- show ospf interfaces command.....205
- show ospf neighbors command.....205
- show ospf statistics command.....205
- show ppp address-pool command.....222
- show ppp interface command.....222
- show ppp statistics command.....222
- show ppp summary command.....222
- show pppoe interfaces command.....219
- show pppoe statistics command.....219
- show pppoe version command.....219
- show redundant-power-supply command.....154
- show rip neighbors command.....204
- show rip statistics command.....204
- show route detail command.....202
- show route terse command.....202
- show services rpm active-servers command.....417
 - explanation.....417
- show services rpm probe-results command.....416, 418
 - explanation.....416
- show snmp health-monitor command.....98
- show snmp statistics command.....97
- show system autoinstallation status command.....133
- show system license command.....320
 - explanation.....320
- show system license keys command.....321
- show system license usage command.....320
 - explanation.....320
- show system process command.....156
- show system processes command.....231
- show system services dhcp binding command.....123
- show system services dhcp binding detail
 - command.....123
- show system services dhcp client command.....124
- show system services dhcp client interface
 - command.....124
- show system services dhcp client statistics
 - command.....124

show system services dhcp conflict command.....	104
show system services dhcp global command.....	122
show system services dhcp relay-statistics	
command.....	126
explanation.....	126
show system storage command.....	151, 152
show system uptime command.....	151, 152
show system users command.....	151, 152
show version command.....	151, 152
show forwarding-options command.....	391
signature update, IDP, license.....	314
Simple Network Management Protocol <i>See</i> SNMP	
SLARP, for autoinstallation.....	132
SMI (Structure of Management Information).....	86
Snapshot page.....	264
snapshots	
configuring for failure snapshot storage.....	268
to replace internal CompactFlash card, for multiple	
devices (CLI).....	267
to replace primary CompactFlash card, for	
multiple devices (J-Web).....	265
SNMP (Simple Network Management Protocol)	
agents <i>See</i> SNMP agents	
architecture.....	85
communities <i>See</i> SNMP communities	
controlling access (configuration editor).....	96, 97
get requests.....	86
health monitor <i>See</i> SNMP health monitor	
managers.....	85
MIBs <i>See</i> MIBs	
on Gigabit Ethernet interfaces.....	85
overview.....	85
preparation.....	88
Quick Configuration.....	88
set requests.....	86
spoofed traps.....	87
support on J Series Services Routers.....	19
support on SRX100, SRX210 devices.....	5
support on SRX3400 and SRX3600 devices.....	15
support on SRX5600 and SRX5800 devices.....	15
system identification (configuration editor).....	93
traps <i>See</i> SNMP traps	
views (configuration editor).....	96
SNMP agents.....	85
configuring (configuration editor).....	94
verifying.....	97
SNMP communities	
creating (configuration editor).....	94
description.....	86
Quick Configuration.....	90
SNMP health monitor	
description.....	87
Quick Configuration.....	88
verifying.....	98
SNMP managers.....	85
SNMP page.....	89
SNMP traps	
automating response to with event policies.....	140
creating groups for (configuration editor).....	95
initiation by event policy, overview.....	141
initiation by event policy, setting (configuration	
editor).....	143
overview.....	87
performance monitoring <i>See</i> RPM probes	
Quick Configuration.....	90
spoofed traps.....	87
software	
halting immediately (CLI)	272
halting immediately (J-Web)	270
upgrades <i>See</i> upgrades	
spoofed SNMP traps.....	87
SRC application.....	23
SRX Series.....	323
alarms.....	239
automating operations with scripts.....	135
automating troubleshooting with scripts and event	
policies.....	135
licenses.....	313
managing user authentication.....	45
monitoring	147
network management.....	85
packet capture.....	381
performance monitoring.....	395
system log messages.....	229
SRX Series Services Gateway	
licenses.....	314
SRX100 devices	
supported features.....	3
SRX100 Memory Upgrade license.....	314
SRX210 devices	
supported features.....	3
SRX240 devices	
supported features.....	3
SRX3400 devices	
supported features.....	13
SRX3600 devices	
supported features.....	13
SRX5600 devices	
supported features.....	13
SRX5800 devices	
supported features.....	13
SRX650 devices	
supported features.....	9
SSH	
accessing remote accounts (CLI).....	63
setting login retry limits.....	64
ssh command.....	63
options.....	63
SSL (Secure Sockets Layer)	
enabling secure access (Quick Configuration).....	39
management access.....	38
verifying SSL configuration.....	43

SSL 3.0 option, disabling on Internet Explorer for worldwide version of JUNOS Software.....	25
SSL access, establishing.....	37
SSL certificates	
adding (configuration editor).....	42
adding (Quick Configuration).....	41
generating.....	39
sample configuration.....	43
support on J Series Services Routers.....	19
support on SRX100, SRX210 and SRX240 devices.....	5
support on SRX3400 and SRX3600 devices.....	14
support on SRX5600 and SRX5800 devices.....	14
support on SRX650 devices.....	11
verifying SSL configuration.....	43
startup	
J-Web interface.....	25
JUNOS CLI.....	29
statements, configuration types.....	31
statistics	
BGP.....	206
interfaces.....	373
LSP.....	217
OSPF.....	205
performance monitoring.....	398
PPPoE.....	220
RIP.....	204
RPM, description.....	398
RPM, monitoring.....	419
RPM, verifying.....	416
status	
autoinstallation.....	133
BGP.....	207
license key.....	318
OSPF interfaces.....	205
OSPF neighbors.....	205
RIP neighbors.....	204
storage media	
configuring boot devices.....	263
Structure of Management Information (SMI).....	86
super-user login class permissions.....	47
superuser login class permissions.....	47
support, technical <i>See</i> technical support	
supported features	
on J Series devices.....	17
on SRX100, SRX210, and SRX240 devices.....	3
on SRX3400 and SRX3600 devices.....	13
on SRX5600 and SRX5800 devices.....	13
on SRX650 devices.....	9
syntax conventions.....	xxiv
syslog <i>See</i> system logs	
system log messages	
/var/log directory.....	234
capturing in a file (configuration editor).....	234
destinations.....	231, 232, 235

displaying at a terminal (configuration editor).....	235
event viewer.....	236
facilities.....	232
monitoring (Quick Configuration).....	236
overview.....	231
preparation.....	233
sending messages to a file (configuration editor).....	234
sending messages to a terminal (configuration editor).....	235
severity levels.....	232
support on J Series Services Routers.....	19
support on SRX100, SRX210 and SRX240 devices.....	6
support on SRX3400 and SRX3600 devices.....	15
support on SRX5600 and SRX5800 devices.....	15
support on SRX650 devices.....	11
system logs	
archiving.....	236
control plane logs.....	233
data plane logs.....	233
destinations for log files.....	231
disabling.....	236
event triggers for SNMP traps, setting in event policies.....	143
file cleanup (CLI).....	328
file cleanup (J-Web).....	324
functions.....	231
logging facilities.....	232
logging severity levels.....	232
messages <i>See</i> system log messages	
monitoring.....	373
overview.....	231
redundant syslog server.....	232
remote syslog server.....	235
system management	
automating.....	135
<i>See also</i> commit scripts; event policies;	
operation scripts	
displaying log and trace file contents.....	373
login classes.....	47, 56
preparation.....	50
Quick Configuration.....	50
system logs.....	229
template accounts.....	50, 59
user accounts.....	46, 58
user authentication.....	46

T

T1 ports	
alarm conditions and configuration options.....	242
configuring alarms on.....	245

T3 ports	
alarm conditions and configuration options.....	244
configuring alarms on.....	245
TACACS +	
adding a server (Quick Configuration).....	50
authentication (configuration editor).....	54
order of user authentication (configuration editor).....	56
secret (configuration editor).....	55
specifying for authentication (Quick Configuration).....	51
taskbar.....	26
TCP RPM probes	
CoS classification, destination interface requirement.....	409
CoS classification, use with caution.....	409
description.....	397
server port.....	405
setting.....	409
verifying servers.....	417
technical support	
contacting JTAC.....	xxvi
Telnet	
accessing remote accounts (CLI).....	62
setting login retry limits.....	64
telnet	
reverse.....	65
reverse SSH.....	66
telnet command.....	63
options.....	63
Telnet session.....	63
template accounts	
description.....	50
local accounts (configuration editor).....	61
remote accounts (configuration editor).....	60
temporary files	
cleaning up (CLI).....	328
cleaning up (J-Web).....	324
downloading (J-Web).....	325
for packet capture.....	384
terminal session, sending system log messages to.....	235
terminal type, setting	36
terminology	
alarms.....	239
autoinstallation.....	127
DHCP.....	101
diagnostic.....	335
monitoring.....	148
packet capture.....	381
RPM.....	395
secure Web access.....	37
system logs.....	229
USB modems.....	67
user authentication.....	45
tests <i>See</i> RPM	
TFTP, for autoinstallation.....	129
threshold	
falling.....	87
rising.....	87
SNMP health monitor.....	87
threshold values, for RPM probes <i>See</i> RPM probes	
time to live <i>See</i> TTL	
timestamps	
for RPM probes <i>See</i> RPM probe timestamps	
suppressing in packet headers, in captured packets.....	357
suppressing in packet headers, in traffic monitoring.....	376
trace files	
monitoring.....	373
multicast, monitoring.....	372
traceroute	
CLI command.....	366
indications.....	353
J-Web tool.....	350
results.....	353
support on J Series Services Routers.....	18
support on SRX100, SRX210 and SRX240 devices.....	4
support on SRX3400 and SRX3600 devices.....	14
support on SRX5600 and SRX5800 devices.....	14
support on SRX650 devices.....	10
TTL increments.....	350
traceroute command.....	366
options.....	366
traceroute monitor	
CLI command.....	367
traceroute monitor command.....	367
options.....	367
results.....	368
Traceroute page.....	352
field summary.....	352
traffic	
analyzing with packet capture.....	381
multicast, tracking.....	370
tracking with J-Web traceroute.....	350
tracking with the traceroute command.....	365
traps <i>See</i> SNMP traps	
triggers for SNMP traps, setting in event policies.....	143
Trivial File Transfer Protocol (TFTP), for autoinstallation.....	129
troubleshooting	
automating with event policies.....	140
operation scripts.....	138
<i>See also</i> diagnosis; operation scripts	
packet capture for analysis.....	381
<i>See also</i> diagnosis; packet capture	
SNMP health monitor.....	87
TTL (time to live)	
default, in multicast path-tracking queries.....	370
in ping requests.....	345

increments, in traceroute packets.....	350
threshold, in multicast trace results.....	371
total, in multicast trace results.....	372
types of configuration statements.....	31

U

UDP RPM probes	
CoS classification, destination interface	
requirement.....	409
CoS classification, use with caution.....	409
description.....	397
server port.....	405
setting.....	409
verifying servers.....	417
umd0.....	68
unauthorized login class permissions.....	47
Unified Threat Management (UTM) license.....	314
universal serial bus <i>See</i> USB	
updating	
licenses (CLI).....	316
upgrade and reboot options	
support on J Series Services Routers.....	20
support on SRX100, SRX210 and SRX240	
devices.....	6
support on SRX3400 and SRX3600 devices.....	15
support on SRX5600 and SRX5800 devices.....	15
support on SRX650 devices.....	11
upgrades	
downloading.....	254
installing (CLI).....	257
installing by uploading.....	256
installing from remote server.....	255
overview.....	252
requirements.....	252, 253
Upload package page.....	257
field summary.....	257
URLs	
Juniper Networks enterprise MIBs.....	86
software downloads.....	254
standard MIBs.....	86
USB (universal serial bus)	
configuring.....	267
configuring for failure snapshot storage.....	268
USB modem connections	
adding an interface.....	71
CHAP on dialer interfaces (configuration	
editor).....	75
configuring device end.....	71
configuring dial-up modem at user end.....	77
connecting device end.....	71
connecting dial-up modem at user end.....	78
connecting to user end.....	77
dial-in (configuration editor).....	74
dialer interface <i>See</i> dialer interface, USB modem	
interface naming conventions.....	68

overview.....	70
requirements.....	71
USB modem interface types.....	68
verifying dialer interfaces.....	82
verifying USB modem interfaces.....	81
USB modem interfaces	
CHAP on dialer interfaces (configuration	
editor).....	75
dial-in (configuration editor).....	74
dialer interface <i>See</i> dialer interface, USB modem	
interface types.....	68
verifying USB modem interfaces.....	81
USB modem remote management	
support on SRX210 devices.....	6
USB modems	
administering.....	78
AT commands.....	69
AT commands, modifying.....	79
configuration overview.....	70
connecting at device end.....	71
connecting at user end.....	77
default modem initialization commands.....	69
default modem initialization commands,	
modifying.....	79
initialization by device.....	69
MultiModem.....	67
overview.....	68
<i>See also</i> dialer interface, for USB modem; USB	
modem connections	
recommended modem.....	67
resetting.....	80
support on J Series Services Routers.....	20
verifying.....	80
user accounts	
authentication order (configuration editor).....	55
contents.....	46
creating (configuration editor).....	59
for local users.....	60
for remote users.....	59
predefined login classes.....	47
templates for.....	50, 59
<i>See also</i> template accounts	
user interfaces	
JUNOScope application.....	23
overview.....	23
preparation.....	25
SRC application.....	23
support on J Series Services Routers.....	20
support on SRX100, SRX210 and SRX240	
devices.....	6
support on SRX3400 and SRX3600 devices.....	15
support on SRX5600 and SRX5800 devices.....	15
support on SRX650 devices.....	12
user logging facility.....	232

username	
description.....	47
specifying (Quick Configuration).....	51
users	
access privileges.....	47, 56
accounts <i>See</i> user accounts	
adding (Quick Configuration).....	51
login classes.....	47, 56
predefined login classes.....	47
template accounts <i>See</i> template accounts	
usernames.....	47
UTM license.....	314

V

verification	
active licenses.....	320
alarm configurations.....	247
autoinstallation.....	133
captured packets.....	392
destination path (J-Web).....	350
DHCP server operation.....	125
DHCP statistics.....	126
dialer interfaces.....	82
firewall filter for packet capture.....	392
host reachability (CLI).....	359
host reachability (J-Web).....	342
license usage.....	320
licenses	319
LSPs (J-Web).....	345
packet capture.....	391
RPM configuration.....	415
RPM probe servers.....	417
RPM statistics.....	416
secure access.....	43
selective stateless packet-based services	
.....	298, 307
SNMP.....	97
SNMP health monitor.....	98
traceroute command.....	365
traceroute monitor command.....	365
tracing multicast paths.....	370
USB modem interfaces.....	81
version	
PPPoE, information about.....	221
version, license key.....	318
views, SNMP.....	96
VPNs (virtual private networks), DHCP support on	
interfaces.....	104

W

warning logging severity.....	232
Web access, secure <i>See</i> secure access	
Web browser, modifying Internet Explorer for	
worldwide version of JUNOS Software.....	25

windows, J-Web, unpredictable results with	
multiple.....	27
working directory, setting.....	35
world-readable statement.....	236

X

XML <i>See</i> commit scripts; operation scripts	
XSLT <i>See</i> commit scripts; operation scripts	

Y

yellow alarms <i>See</i> minor alarms	
---------------------------------------	--