



J-series™ Services Router

Administration Guide

Release 8.0

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-016297-01, Revision 1

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, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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.

Copyright © 2006, Juniper Networks, Inc. All rights reserved.

J-series™ Services Router Administration Guide, Release 8.0
Copyright © 2006, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Nidhi Bhargava, Michael Bushong, Maya Devi, Taffy Everts, Jerry Isaac, Archana Maheshwari, Hareesh Kumar Kozhippurath Narayana Panicker, Laura Phillips, Frank Reade, Swapna Steiger, and Selvakumar T. S.
Editing: Taffy Everts and Stella Hackell
Illustration: Faith Bradford Brown and Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
29 June 2006—Revision 1.

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 Web site 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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 the Embedded Software on non-Juniper equipment; (j) use the 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 NONINFRINGEMENT. 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

xv

Part 1

Configuring a Services Router for Administration

Chapter 1	Managing User Authentication and Access	3
Chapter 2	Configuring SNMP for Network Management	31
Chapter 3	Configuring the Router as a DHCP Server	47
Chapter 4	Automating Network Operations and Troubleshooting	65

Part 2

Monitoring a Services Router

Chapter 5	Monitoring the Router and Routing Operations	77
Chapter 6	Monitoring Events and Managing System Log Files	129
Chapter 7	Configuring and Monitoring Alarms	143

Part 3

Managing Services Router Software

Chapter 8	Performing Software Upgrades and Reboots	159
Chapter 9	Managing Files	183

Part 4

Diagnosing Performance and Network Problems

Chapter 10	Using Services Router Diagnostic Tools	197
------------	--	-----

Chapter 11	Configuring Packet Capture ..	245
Chapter 12	Configuring RPM Probes ..	259
Part 5	Index	

Table of Contents

About This Guide xv

Objectives	xv
Audience.....	xvi
Document Conventions	xvi
Related Juniper Networks Documentation.....	xviii
Documentation Feedback.....	xx
Requesting Support.....	xx

Part 1

Configuring a Services Router for Administration

Chapter 1

Managing User Authentication and Access 3

User Authentication Terms.....	3
User Authentication Overview	4
User Authentication.....	4
User Accounts	4
Login Classes	5
Permission Bits	5
Denying or Allowing Individual Commands	7
Template Accounts.....	8
Before You Begin.....	8
Managing User Authentication with Quick Configuration	8
Adding a RADIUS Server for Authentication	8
Adding a TACACS+ Server for Authentication	10
Configuring System Authentication.....	12
Adding New Users	14
Managing User Authentication with a Configuration Editor	16
Setting Up RADIUS Authentication	17
Setting Up TACACS+ Authentication	18
Configuring Authentication Order	19
Controlling User Access.....	21
Defining Login Classes.....	21
Creating User Accounts	23
Setting Up Template Accounts	24
Creating a Remote Template Account	24
Creating a Local Template Account	25
Securing the Console Port.....	26
Accessing Remote Devices with the CLI	27
Using the telnet Command	27
Using the ssh Command	28

Configuring Password Retry Limits for Telnet and SSH Access	29
---	----

Chapter 2 Configuring SNMP for Network Management 31

Network Management Overview	31
Managers and Agents.....	31
SMI, MIBs, and OIDs.....	32
Standard and Enterprise MIBs	32
SNMP Requests	32
SNMP Communities	32
SNMP Traps.....	33
SNMP Health Monitor.....	33
Before You Begin.....	34
Configuring SNMP with Quick Configuration.....	34
Configuring SNMP with a Configuration Editor	39
Defining System Identification Information (Required).....	39
Configuring SNMP Agents and Communities (Required)	40
Managing SNMP Trap Groups (Required)	41
Controlling Access to MIBs (Optional)	42
Verifying the SNMP Configuration.....	43
Verifying SNMP Agent Configuration	44
Verifying SNMP Health Monitor Configuration	44

Chapter 3 Configuring the Router as a DHCP Server 47

DHCP Terms	47
DHCP Overview.....	48
DHCP Options.....	49
Compatibility with Autoinstallation.....	49
Conflict Detection and Resolution	49
Interface Restrictions	49
Before You Begin.....	50
Configuring the DHCP Server with Quick Configuration	50
Configuring the DHCP Server with a Configuration Editor	56
Verifying a DHCP Server Configuration	59
Displaying a DHCP Server Configuration	60
Verifying the DHCP Binding Database	60
Verifying DHCP Server Operation	62
Displaying DHCP Statistics	63

Chapter 4 Automating Network Operations and Troubleshooting 65

Defining and Enforcing Configuration Rules with Commit Scripts	65
Commit Script Overview	65
Enabling Commit Scripts.....	66
Disabling Commit Scripts	67
Automating Network Management and Troubleshooting with Operation Scripts	68
Operation Script Overview	68
Enabling Operation Scripts.....	69

Executing Operation Scripts	70
Disabling Operation Scripts	70
Running Self-Diagnostics with Event Policies	71
Event Policy Overview	71
Configuring Event Policies	72

Part 2

Monitoring a Services Router

Chapter 5

Monitoring the Router and Routing Operations 77

Monitoring Terms	77
Monitoring Overview	78
Monitoring Tools Overview	78
Filtering Command Output	82
Before You Begin	83
Using the Monitoring Tools	83
Monitoring System Properties	84
Monitoring System Process Information	87
Monitoring the Chassis	87
Monitoring the Interfaces	89
Monitoring Routing Information	91
Monitoring Routing Information	91
Monitoring BGP Routing Information	93
Monitoring OSPF Routing Information	94
Monitoring RIP Routing Information	96
Monitoring DLSw Routing Information	97
Monitoring Class-of-Service Performance	98
Monitoring CoS Interfaces	99
Monitoring CoS Classifiers	100
Monitoring CoS Value Aliases	101
Monitoring CoS RED Drop Profiles	101
Monitoring CoS Forwarding Classes	102
Monitoring CoS Rewrite Rules	103
Monitoring CoS Scheduler Maps	104
Monitoring MPLS Traffic Engineering Information	106
Monitoring MPLS Interfaces	106
Monitoring MPLS LSP Information	107
Monitoring MPLS LSP Statistics	108
Monitoring RSVP Session Information	109
Monitoring MPLS RSVP Interfaces Information	110
Monitoring Service Sets	111
Monitoring Firewalls	112
Monitoring Stateful Firewall Statistics	112
Monitoring Stateful Firewall Filters	114
Monitoring Firewall Intrusion Detection Services (IDS)	114
Monitoring IPSec Tunnels	116
Monitoring NAT Pools	118
Monitoring DHCP	118
Monitoring RPM Probes	120
Monitoring PPP	123
Monitoring PPPoE	124

Chapter 6	Monitoring Events and Managing System Log Files	129
	System Log Message Terms	129
	System Log Messages Overview	130
	System Log Message Destinations	131
	System Log Facilities and Severity Levels	131
	Regular Expressions	132
	Before You Begin	134
	Configuring System Log Messages with a Configuration Editor	134
	Sending System Log Messages to a File	134
	Sending System Log Messages to a User Terminal	135
	Archiving System Logs	136
	Disabling System Logs	136
	Monitoring System Log Messages with the J-Web Event Viewer	137
	Filtering System Log Messages	138
	Viewing System Log Messages	140
Chapter 7	Configuring and Monitoring Alarms	143
	Alarm Terms	143
	Alarm Overview	144
	Alarm Types	144
	Alarm Severity	145
	Alarm Conditions	145
	Interface Alarm Conditions	145
	Chassis Alarm Conditions and Corrective Actions	148
	System Alarm Conditions and Corrective Actions	149
	Before You Begin	150
	Configuring Alarms with a Configuration Editor	150
	Checking Active Alarms	152
	Verifying the Alarms Configuration	154
	Displaying Alarm Configurations	154
Part 3	Managing Services Router Software	
Chapter 8	Performing Software Upgrades and Reboots	159
	Upgrade and Downgrade Overview	160
	Upgrade Software Packages	160
	Recovery Software Packages	160
	Before You Begin	161
	Downloading Software Upgrades from Juniper Networks	162
	Installing Software Upgrades	162
	Installing Software Upgrades with the J-Web Interface	163
	Installing Software Upgrades from a Remote Server	163
	Installing Software Upgrades by Uploading Files	164
	Installing Software Upgrades with the CLI	166
	Downgrading the Software	166

Downgrading the Software with the J-Web Interface.....	167
Downgrading the Software with the CLI	167
Configuring Boot Devices	167
Configuring a Boot Device for Backup with the J-Web Interface	168
Configuring a Boot Device for Backup with the CLI	171
Configuring a Boot Device to Receive Software Failure Memory Snapshots.....	173
Recovering Primary Boot Devices	173
Why Compact Flash Recovery Might Be Necessary	174
Recommended Recovery Hardware and Software	174
Configuring Primary Compact Flash Recovery	175
Rebooting or Halting a Services Router	177
Rebooting or Halting a Services Router with the J-Web Interface	177
Rebooting a Services Router with the CLI.....	180
Halting a Services Router with the CLI	180

Chapter 9 Managing Files 183

Before You Begin.....	183
Managing Files with the J-Web Interface.....	183
Cleaning Up Files	183
Downloading Files	186
Deleting Files.....	188
Cleaning Up Files with the CLI.....	190
Encrypting and Decrypting Configuration Files	191
Encrypting Configuration Files.....	191
Decrypting Configuration Files	193
Modifying the Encryption Key	193

Part 4 Diagnosing Performance and Network Problems

Chapter 10

Using Services Router Diagnostic Tools

197

Diagnostic Terms	197
Diagnostic Tools Overview	198
J-Web Diagnostic Tools Overview	198
CLI Diagnostic Commands Overview	199
MPLS Connection Checking	201
Before You Begin	202
General Preparation	203
Ping MPLS Preparation	203
MPLS Enabled	203
Loopback Address	203
Source Address for Probes	203
Pinging Hosts from the J-Web Interface	203
Using the J-Web Ping Host Tool	204
Ping Host Results and Output Summary	207
Checking MPLS Connections from the J-Web Interface	209
Using the J-Web Ping MPLS Tool	209
Ping MPLS Results and Output	212

Tracing Unicast Routes from the J-Web Interface	213
Using the J-Web Traceroute Tool	214
Traceroute Results and Output Summary	216
Capturing and Viewing Packets with the J-Web Interface	217
Using J-Web Packet Capture	218
Packet Capture Results and Output Summary	222
Using CLI Diagnostic Commands	223
Pinging Hosts from the CLI	223
Checking MPLS Connections from the CLI	225
Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs	226
Pinging Layer 3 VPNs	227
Pinging Layer 2 VPNs	227
Pinging Layer 2 Circuits	229
Tracing Unicast Routes from the CLI	229
Using the traceroute Command	230
Using the traceroute monitor Command	231
Tracing Multicast Routes from the CLI	233
Using the mtrace from-source Command	233
Using the mtrace monitor Command	235
Displaying Log and Trace Files from the CLI	236
Monitoring Interfaces and Traffic from the CLI	237
Using the monitor interface Command	237
Using the monitor traffic Command	239

Chapter 11

Configuring Packet Capture 245

Packet Capture Terms	245
Packet Capture Overview	246
Packet Capture on Router Interfaces	247
Firewall Filters for Packet Capture	248
Packet Capture Files	248
Analysis of Packet Capture Files	248
Before You Begin	249
Configuring Packet Capture with a Configuration Editor	249
Enabling Packet Capture (Required)	249
Configuring Packet Capture on an Interface (Required)	250
Configuring a Firewall Filter for Packet Capture (Optional)	251
Disabling Packet Capture	253
Deleting Packet Capture Files	253
Changing Encapsulation on Interfaces with Packet Capture Configured	254
Verifying Packet Capture	255
Displaying a Packet Capture Configuration	255
Displaying a Firewall Filter for Packet Capture Configuration	256
Verifying Captured Packets	256

Chapter 12

Configuring RPM Probes 259

RPM Terms	259
RPM Overview	260
RPM Probes	260

RPM Tests.....	261
Probe and Test Intervals.....	261
RPM Statistics	261
RPM Thresholds and Traps.....	262
RPM for BGP Monitoring	262
Before You Begin.....	263
Configuring RPM with Quick Configuration	263
Configuring RPM with a Configuration Editor	270
Configuring Basic RPM Probes.....	270
Configuring TCP and UDP Probes	274
Tuning RPM Probes.....	276
Configuring RPM Probes to Monitor BGP Neighbors.....	277
Configuring RPM Probes for BGP Monitoring.....	277
Directing RPM Probes to Select BGP Routers	279
Verifying an RPM Configuration	280
Verifying RPM Statistics	281
Verifying RPM Probe Servers.....	282

Part 5

Index

Index.....	285
------------	-----

About This Guide

This preface provides the following guidelines for using the *J-series™ Services Router Administration Guide*:

- Objectives on page xv
- Audience on page xvi
- Document Conventions on page xvi
- Related Juniper Networks Documentation on page xviii
- Documentation Feedback on page xx
- Requesting Support on page xx

Objectives

This guide contains instructions for managing users and operations, monitoring network performance, upgrading software, and diagnosing common problems on J-series Services Routers.



NOTE: This guide documents Release 8.0 of the JUNOS software. For additional information about J-series Services Routers—either corrections to or omissions from this guide—see the *J-series Services Router Release Notes* at <http://www.juniper.net>.

J-series Services Router operations are controlled by the JUNOS Internet software. You direct the JUNOS software through either a Web browser or a command-line interface (CLI) to perform the tasks shown in Table 1.

Table 1: Capabilities of J-series Interfaces

J-series Interface	Capabilities
J-Web graphical browser interface	<ul style="list-style-type: none">■ Quick (basic) configuration■ Monitoring, configuration, diagnosis, and management
JUNOS CLI	Monitoring, configuration, diagnosis, and management

J-series Services Router guides provide complete instructions for using the J-Web interface, but they are not a comprehensive resource for using the JUNOS CLI. For CLI information, see the JUNOS software manuals listed in “Related Juniper Networks Documentation” on page xviii.

Although the *J-Web Interface User Guide* provides a useful overview of the J-Web interface, it contains only a subset of J-Web information. We recommend that J-series users consult the J-series Services Router guides, instead.

Audience

This guide is designed for anyone who installs and sets up a J-series Services Router or prepares a site for Services Router installation. The guide is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and the Internet
- Network administrators who install, configure, and manage Internet routers but are unfamiliar with the JUNOS software
- Network administrators who install, configure, and manage products of Juniper Networks

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Document Conventions

Table 2 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.

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

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width typeface	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic typeface</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 sans serif typeface</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Sans serif typeface	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 stub statement at the [edit protocols ospf area <i>area-id</i>] hierarchy level. The console port is labeled CONSOLE.
< > (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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	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 <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		

Convention	Description	Examples
Bold typeface	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 .

Related Juniper Networks Documentation

J-series Services Routers are documented in multiple guides. Although the J-series guides provide instructions for configuring and managing a Services Router with the JUNOS CLI, they are not a comprehensive JUNOS software resource. For complete documentation of the statements and commands described in J-series guides, see the JUNOS software manuals listed in Table 4.

Table 4: J-series Guides and Related JUNOS Software Publications

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
Getting Started Guide for Your Router	
"J-series User Interface Overview"	■ <i>JUNOS CLI User Guide</i>
"Establishing Basic Connectivity"	■ <i>JUNOS System Basics Configuration Guide</i>
"Configuring Autoinstallation"	
J-series Services Router Basic LAN and WAN Access Configuration Guide	
"Using Services Router Configuration Tools"	<ul style="list-style-type: none"> ■ <i>JUNOS CLI User Guide</i> ■ <i>JUNOS System Basics Configuration Guide</i>
"Interfaces Overview"	■ <i>JUNOS Network Interfaces Configuration Guide</i>
"Configuring DS1, DS3, Ethernet, and Serial Interfaces"	■ <i>JUNOS Interfaces Command Reference</i>
"Configuring Digital Subscriber Line Interfaces"	
"Configuring Point-to-Point Protocol over Ethernet"	
"Configuring ISDN"	
"Configuring Link Services Interfaces"	<ul style="list-style-type: none"> ■ <i>JUNOS Services Interfaces Configuration Guide</i> ■ <i>JUNOS System Basics and Services Command Reference</i>

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
“Routing Overview”	■ <i>JUNOS Routing Protocols Configuration Guide</i>
“Configuring Static Routes”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring a RIP Network”	
“Configuring an OSPF Network”	
“Configuring the IS-IS Protocol”	
“Configuring BGP Sessions”	
J-series Services Router Advanced WAN Access Configuration Guide	
“Multiprotocol Label Switching Overview”	■ <i>JUNOS MPLS Applications Configuration Guide</i>
“Configuring Signaling Protocols for Traffic Engineering”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring Virtual Private Networks”	■ <i>JUNOS VPNs Configuration Guide</i>
“Configuring CLNS VPNs”	
“Configuring IPSec for Secure Packet Exchange”	■ <i>JUNOS System Basics Configuration Guide</i>
	■ <i>JUNOS Services Interfaces Configuration Guide</i>
	■ <i>JUNOS System Basics and Services Command Reference</i>
“Multicast Overview”	■ <i>JUNOS Multicast Protocols Configuration Guide</i>
“Configuring a Multicast Network”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring Data Link Switching”	■ <i>JUNOS Services Interfaces Configuration Guide</i>
	■ <i>JUNOS System Basics and Services Command Reference</i>
“Policy Framework Overview”	■ <i>JUNOS Policy Framework Configuration Guide</i>
“Configuring Routing Policies”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring NAT”	■ <i>JUNOS Network Interfaces Configuration Guide</i>
“Configuring Stateful Firewall Filters and NAT”	■ <i>JUNOS Policy Framework Configuration Guide</i>
“Configuring Stateless Firewall Filters”	■ <i>JUNOS Services Interfaces Configuration Guide</i>
	■ <i>JUNOS System Basics and Services Command Reference</i>
	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Class-of-Service Overview”	■ <i>JUNOS Class of Service Configuration Guide</i>
“Configuring Class of Service”	■ <i>JUNOS System Basics and Services Command Reference</i>
J-series Services Router Administration Guide	
“Managing User Authentication and Access”	<i>JUNOS System Basics Configuration Guide</i>
“Configuring SNMP for Network Management”	<i>JUNOS Network Management Configuration Guide</i>
“Configuring the Router as a DHCP Server”	<i>JUNOS System Basics Configuration Guide</i>
“Automating Network Operations and Troubleshooting”	<i>JUNOS Configuration and Diagnostic Automation Guide</i>

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
"Monitoring the Router and Routing Operations"	<ul style="list-style-type: none"> ■ <i>JUNOS System Basics and Services Command Reference</i> ■ <i>JUNOS Interfaces Command Reference</i> ■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
"Monitoring Events and Managing System Log Files"	<i>JUNOS System Log Messages Reference</i>
"Configuring and Monitoring Alarms"	<i>JUNOS System Basics Configuration Guide</i>
"Performing Software Upgrades and Reboots"	<i>JUNOS Installation and Upgrade Guide</i>
"Using Services Router Diagnostic Tools"	<ul style="list-style-type: none"> ■ <i>JUNOS System Basics and Services Command Reference</i> ■ <i>JUNOS Interfaces Command Reference</i> ■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
"Configuring Packet Capture"	<i>JUNOS Services Interfaces Configuration Guide</i>
"Configuring RPM Probes"	<i>JUNOS System Basics and Services Command Reference</i>

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 <http://www.juniper.net/techpubs/docbug/docbugreport.html>. 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

Requesting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Part 1

Configuring a Services Router for Administration

- Managing User Authentication and Access on page 3
- Configuring SNMP for Network Management on page 31
- Configuring the Router as a DHCP Server on page 47
- Automating Network Operations and Troubleshooting on page 65

Chapter 1

Managing User Authentication and Access

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.

This chapter contains the following topics. For more information about system management, see the *JUNOS System Basics Configuration Guide*.

- User Authentication Terms on page 3
- User Authentication Overview on page 4
- Before You Begin on page 8
- Managing User Authentication with Quick Configuration on page 8
- Managing User Authentication with a Configuration Editor on page 16
- Securing the Console Port on page 26
- Accessing Remote Devices with the CLI on page 27
- Configuring Password Retry Limits for Telnet and SSH Access on page 29

User Authentication Terms

Before performing system management tasks, become familiar with the terms defined in Table 5.

Table 5: 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 4
- User Accounts on page 4
- Login Classes on page 5
- Template Accounts on page 8

User Authentication

The 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 Services Router.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router using Telnet. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the router, and the server runs on a remote network system.

You can configure the router to use RADIUS or TACACS+ authentication, or both, to validate users who attempt to access the router. If you set up both authentication methods, you also can configure which the router will try first.

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 “Managing User Authentication with Quick Configuration” on page 8 and “Managing User Authentication with a Configuration Editor” on page 16. After

you have created an account, the router 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 Getting Started Guide for your router. For each user account, you can define the following:

- Username—Name that identifies the user. It must be unique within the router. 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 router. 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 7.
- Authentication method or methods and passwords that the user can use to access the router—You can use SSH or an MD5 password, or you can enter a plain-text password that the 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. With login classes, you define the following:

- Access privileges users have when they are logged into the router. For more information, see "Permission Bits" on page 5.
- Commands and statements that users can and cannot specify. For more information, see "Denying or Allowing Individual Commands" on page 7.
- How long a login session can be idle before it times out and the user is logged off.

You can define any number of login classes. You then apply one login class to an individual user account. The software contains a few predefined login classes, which are listed in Table 7. The predefined login classes cannot be modified.

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 6).

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 6: Permission Bits for Login Classes

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

Table 6: Permission Bits for Login Classes (continued)

Permission Bit	Access
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 router 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.

Table 7: Predefined Login Classes

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

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, the 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 router, 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 router selects the appropriate local user template locally configured on the router. If a local user template does not exist for the authenticated user, the router defaults to the remote template.

For more information, see “Setting Up Template Accounts” on page 24.

Before You Begin

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

Managing User Authentication with Quick Configuration

This section contains the following topics:

- Adding a RADIUS Server for Authentication on page 8
- Adding a TACACS+ Server for Authentication on page 10
- Configuring System Authentication on page 12
- Adding New Users on page 14

Adding a RADIUS Server for Authentication

You can use the Users Quick Configuration page for RADIUS servers to configure a RADIUS server for system authentication. This Quick Configuration page allows you to specify the IP address and secret (password) of the RADIUS server.

Figure 1 shows the Users Quick Configuration page for RADIUS servers.

Figure 1: Users Quick Configuration Page for RADIUS Servers

The screenshot displays the Juniper J-Web interface for a ROUTER - J4300. The top navigation bar includes links for Monitor, Configuration, Diagnose, Manage, Events, Logged in as: regress, Help, About, and Logout. The left sidebar shows a tree view with 'Quick Configuration' selected. The main content area is titled 'Quick Configuration' and 'Users'. A link 'Add a RADIUS Server' is visible. Below this, the 'RADIUS Server' section contains three input fields: 'RADIUS Server Address', 'RADIUS Server Secret', and 'Verify RADIUS Server Secret'. At the bottom of this section are 'OK' and 'Cancel' buttons. The footer contains copyright information for 2004-2005 and the Juniper logo.

To configure a RADIUS server with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > Users**.
2. Under RADIUS servers, click **Add** to configure a RADIUS server.
3. Enter information into the Users Quick Configuration page for RADIUS servers, as described in Table 8.
4. Click one of the following buttons on the Users Quick Configuration page for RADIUS servers:
 - To apply the configuration and return to the Users Quick Configuration page, click **OK**.
 - To cancel your entries and return to the Users Quick Configuration page, click **Cancel**.

Table 8: Users Quick Configuration for RADIUS Servers Summary

Field	Function	Your Action
RADIUS Server		
RADIUS Server Address (required)	Identifies the IP address of the RADIUS server.	Type the RADIUS server's 32-bit IP address, in dotted decimal notation.
RADIUS Server Secret (required)	The secret (password) of the RADIUS server.	Type the secret (password) of the RADIUS server. Secrets can contain spaces. The secret used must match that used by the RADIUS server.
Verify RADIUS Server Secret (required)	Verifies the secret (password) of the RADIUS server is entered correctly.	Retype the secret of the RADIUS server.

Adding a TACACS+ Server for Authentication

You can use the Users Quick Configuration page for TACACS + servers to configure a TACACS + server for system authentication. This Quick Configuration page allows you to specify the IP address and secret of the TACACS + server.

Figure 2 shows the Users Quick Configuration page for TACACS + servers.

Figure 2: Users Quick Configuration Page for TACACS+ Servers

Juniper NETWORKS ROUTER - J4300

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

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

Quick Configuration

Users [Add a TACACS+ Server](#)

TACACS+ Server

* TACACS+ Server Address

* TACACS+ Server Secret

* Verify TACACS+ Server Secret

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved](#). [Trademark Notice](#). [Privacy](#). Juniper Your Net.

To configure a TACACS+ server with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > Users**.
2. Under TACACS+ servers, click **Add** to configure a TACACS+ server.
3. Enter information into the Users Quick Configuration page for TACACS+ servers, as described in Table 9.
4. Click one of the following buttons on the Users Quick Configuration page for TACACS+ servers:
 - To apply the configuration and return to the Users Quick Configuration page, click **OK**.
 - To cancel your entries and return to the Users Quick Configuration page, click **Cancel**.

Table 9: Users Quick Configuration for TACACS+ Servers Summary

Field	Function	Your Action
TACACS+ Server		
TACACS + Server Address (required)	Identifies the IP address of the TACACS + server.	Type the TACACS + server's 32-bit IP address, in dotted decimal notation.
TACACS + Server Secret (required)	The secret (password) of the TACACS + server.	Type the secret (password) of the TACACS + server. Secrets can contain spaces. The secret used must match that used by the TACACS + server.
Verify TACACS + Server Secret (required)	Verifies the secret (password) of the TACACS + server is entered correctly.	Retype the secret of the TACACS + server.

Configuring System Authentication

On the Users Quick Configuration page, you can configure the authentication methods the Services Router uses to verify that a user can gain access. For each login attempt, the router 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.

Figure 3 shows the Users Quick Configuration page.

Figure 3: Users Quick Configuration Page

Juniper
NETWORKS

ROUTER - J4300

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

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

Quick Configuration

Users

Users

	Username	Full Name	Login Class
<input type="checkbox"/>	regress		superuser
<input type="checkbox"/>	tpe		superuser

[Add...](#) [Delete](#)

Authentication Servers

Authentication Methods

- ☒ RADIUS
- ☒ TACACS+
- ☒ Local Password

RADIUS Servers

	RADIUS Server	Secret Configured
<input type="checkbox"/>	192.168.64.10	Yes
<input type="checkbox"/>	192.168.4.240	Yes

[Add...](#) [Delete](#)

TACACS+ Servers

	TACACS+ Server	Secret Configured
<input type="checkbox"/>	192.168.5.73	Yes

[Add...](#) [Delete](#)

[OK](#) [Cancel](#) [Apply](#)

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved](#). [Trademark Notice](#). [Privacy](#).

Juniper your Net.

To configure system authentication with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > Users**.
2. Under Authentication Servers, select the check box next to each authentication method the router must use when users log in:
 - RADIUS
 - TACACS +
 - Local Password
3. Click one of the following buttons on the Users Quick Configuration page:
 - To apply the configuration and stay in the Users Quick Configuration page, click **Apply**.
 - To apply the configuration and return to the Quick Configuration page, click **OK**.
 - To cancel your entries and return to the Quick Configuration page, click **Cancel**.

Adding New Users

You can use the Users Quick Configuration page for user information to add new users to a Services Router. For each account, you define a login name and password for the user and specify a login class for access privileges.

Figure 4 shows the Quick Configuration page for adding a user.

Figure 4: Add a User Quick Configuration Page

Juniper NETWORKS ROUTER - J4300

Monitor Configuration Diagnose Manage Events Logged in as: regress Help About Logout

Quick Configuration View and Edit History Rescue

Configuration > Quick Configuration > Users

Quick Configuration

Users Add a User

User Information

* Username

Full Name

* Login Class

* Login Password

* Verify Login Password

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

To configure users with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > Users**.
2. Under Users, click **Add** to add a new user.
3. Enter information into the Add a User Quick Configuration page, as described in Table 10.
4. Click one of the following buttons on the Add a User Quick Configuration page:
 - To apply the configuration and return to the Users Quick Configuration page, click **OK**.
 - To cancel your entries and return to the Users Quick Configuration page, click **Cancel**.

Table 10: Add a User Quick Configuration Page Summary

Field	Function	Your Action
User Information		
Username (required)	Name that identifies the user.	Type the username. It must be unique within the router. Do not include spaces, colons, or commas in the username.
Full Name	The user's full name.	Type the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
Login Class (required)	Defines the user's access privilege.	<p>From the list, select the user's login class:</p> <ul style="list-style-type: none"> ■ operator ■ read-only ■ super-user/superuser ■ unauthorized <p>This list also includes any user-defined login classes. For more information, see "Login Classes" on page 5.</p>
Login Password (required)	The login password for this user.	<p>Type the login password for this user. The login password must meet the following criteria:</p> <ul style="list-style-type: none"> ■ 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.
Verify Login Password (required)	Verifies the login password for this user.	Retype the login password for this user.

Managing User Authentication with a Configuration Editor

This section contains the following topics:

- Setting Up RADIUS Authentication on page 17
- Setting Up TACACS+ Authentication on page 18
- Configuring Authentication Order on page 19

- Controlling User Access on page 21
- Setting Up Template Accounts on page 24

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 router. 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 router 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 11.
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 19.
 - To configure a remote user template account, see "Creating a Remote Template Account" on page 24.
 - To configure local user template accounts, see "Creating a Local Template Account" on page 25.

Table 11: 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 Configuration > View and Edit > Edit Configuration. 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.	<p>In the Secret box, type the shared secret of the RADIUS server:</p> <p>Radiussecret1</p>	Set the shared secret of the RADIUS server: set radius-server 172.16.98.1 secret Radiussecret1
Specify the source address to be included in the RADIUS server requests by the router. In most cases, you can use the loopback address of the router.	<p>In the Source address box, type the loopback address of the router:</p> <p>10.0.0.1</p>	Set the router'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 router. 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 router 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 12.
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 19.
 - To configure a remote user template account, see “Creating a Remote Template Account” on page 24.
 - To configure local user template accounts, see “Creating a Local Template Account” on page 25.

Table 12: 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 Configuration > View and Edit > Edit Configuration. 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.	In the Secret box, type the shared secret of the TACACS + server: Tacacssecret1	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 router. In most cases, you can use the loopback address of the router.	In the Source address box, type the loopback address of the router: 10.0.0.1	Set the router'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 13.
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 17.
 - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 18.
 - To configure a remote user template account, see “Creating a Remote Template Account” on page 24.
 - To configure local user template accounts, see “Creating a Local Template Account” on page 25.

Table 13: 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 Configuration > View and Edit > Edit Configuration. 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 21
- Creating User Accounts on page 23

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 23 and “Setting Up Template Accounts” on page 24.

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 5.

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 14.
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 23.
 - To create shared user accounts, see “Setting Up Template Accounts” on page 24.

Table 14: 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 Configuration > View and Edit > Edit Configuration. 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 login class named operator-and-boot with the ability to reboot the router.	<ol style="list-style-type: none"> 1. Next to Class, click Add new entry. 2. Type the name of the login class: operator-and-boot 3. In the Allow commands box, type the request system reboot command enclosed in quotation marks: "request system reboot" 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>
Give the operator-and-boot login class operator privileges.	<ol style="list-style-type: none"> 1. Next to Permissions, click Add new entry. 2. In the Value list, select clear. 3. Click OK. 4. Next to Permissions, click Add new entry. 5. In the Value list, select network. 6. Click OK. 7. Next to Permissions, click Add new entry. 8. In the Value list, select reset. 9. Click OK. 10. Next to Permissions, click Add new entry. 11. In the Value list, select trace. 12. Click OK. 13. Next to Permissions, click Add new entry. 14. In the Value list, select view. 15. Click OK. 	<p>Set the permission bits for the operator-and-boot login class:</p> <p>set class operator-and-boot permissions [clear network reset trace view]</p>

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 17 and “Setting Up TACACS+ Authentication” on page 18.)

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$14c5.$sBopasdFFdssdfFFdsdfs0`.

To create user accounts:

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 15.
3. If you are finished configuring the network, commit the configuration.

Table 15: 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Configure or Edit. 3. Next to Login, click Configure or Edit. 	From the [edit] hierarchy level, enter <code>edit system login</code>
Create a user named <code>cmartin</code> who belongs to the <code>superuser</code> login class.	<ol style="list-style-type: none"> 1. Next to User, click Add new entry. 2. In the User name box, type <code>cmartin</code>. 3. In the Class box, type <code>superuser</code>. 4. Click OK. 	Set the username and the login class for the user: <code>set user cmartin class superuser</code>
Define the encrypted password for <code>cmartin</code> .	<ol style="list-style-type: none"> 1. Next to Authentication, click Configure. 2. In the Encrypted password box, type <code>\$1\$14c5.\$sBopasdFFdssdfFFdsdfs0</code> 3. Click OK. 	Set the encrypted password for <code>cmartin</code> . <code>set user cmartin authentication encrypted-password \$1\$14c5.\$sBopasdFFdssdfFFdsdfs0</code>

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 24
- Creating a Local Template Account on page 25

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, the 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 router.

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 16.
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 17.
 - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 18.
 - To specify a system authentication order, see “Configuring Authentication Order” on page 19.

Table 16: 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 Configuration > View and Edit > Edit Configuration. 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 17.
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 17.
 - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 18.

- To configure a system authentication order, see “Configuring Authentication Order” on page 19.

Table 17: 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 Configuration > View and Edit > Edit Configuration. 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 Services Router to connect to the Routing Engine through an RJ-45 serial cable. From the console port, you can use the CLI to configure the router. By default, the console port is enabled. To secure the console port, you can configure the Services Router 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 Services Router, especially when the router 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 18.
3. If you are finished configuring the network, commit the configuration.

Table 18: 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Configure or Edit. 3. Next to Ports, click Configure or Edit. 4. Next to Console, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system ports console
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. 	Do one of the following: <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 27
- Using the ssh Command on page 28

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-J. To exit from the Telnet session and return to the CLI command prompt, enter quit.

Table 19 describes the telnet command options. For more information, see the *JUNOS System Basics and Services Command Reference*.

Table 19: 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> <logical-router logical-router-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```

Table 20 describes the ssh command options. For more information, see the *JUNOS System Basics and Services Command Reference*.

Table 20: CLI ssh Command Options

Option	Description
bypass-routing	Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.
host	Open an SSH connection to the specified hostname or IP address.
inet	Force the SSH connection to an IPv4 destination.
interface <i>source-interface</i>	Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.
routing-instance <i>routing-instance-name</i>	Use the specified routing instance for the SSH connection.

Table 20: CLI ssh Command Options (continued)

Option	Description
source <i>address</i>	Use the specified source address for the SSH connection.
v1	Force SSH to use version 1 for the connection.
v2	Force SSH to use version 2 for the connection.

Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the Services Router takes 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 21.
3. If you are finished configuring the network, commit the configuration.

Table 21: 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Edit. 3. Next to Login, click Configure or Edit. 4. Next to Retry options, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system login retry-options
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

Chapter 2

Configuring SNMP for Network Management

The Simple Network Management Protocol (SNMP) is a client/server standard that helps you diagnose and monitor network health and statistics.

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

This chapter contains the following topics. For more information about SNMP, see the *JUNOS Network Management Configuration Guide*.

- Network Management Overview on page 31
- Before You Begin on page 34
- Configuring SNMP with Quick Configuration on page 34
- Configuring SNMP with a Configuration Editor on page 39
- Verifying the SNMP Configuration on page 43

Network Management Overview

A network is a complex organization of nodes and processes that must operate reliably and efficiently. Having a single node or link failure in a network can undermine the network's performance and result in a loss of service. Therefore, determining where and when a network failure is occurring is a necessity.

Additionally, gathering statistics about how a network is performing can help you diagnose the overall health of the network and pinpoint bottlenecks so that you can address network growth appropriately.

By querying individual network nodes and receiving triggered updates, SNMP clients are able to provide valuable feedback about the state of a network.

Managers and Agents

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 they 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. 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.

SMI, MIBs, and OIDs

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.

Standard and Enterprise MIBs

A set of MIBs has been defined by the IETF and documented in various RFCs. These MIBs are common across many platforms. Additionally, individual enterprises can create their own set of enterprise-specific MIBs, provided they share the same structure as the standard MIBs. This structure is enforced through the Abstract Syntax Notation (ASN), which is a definition language used to store information.

To download the standard and enterprise MIBs for a Services Router, go to http://www.juniper.net/techpubs/software/index_mibs.html.

SNMP Requests

Information is stored in MIBs, and MIBs are queried by SNMP managers. Managers send SNMP requests to process the information. SNMP requests come in two primary forms: get requests and set requests. These requests are processed by one or more agents on a particular node, and information is retrieved or modified on the MIB. When the agent has processed the request, it generates an SNMP response that either returns retrieved information from the MIB or acknowledges that information has been modified on the MIB.

SNMP Communities

To help ensure that only specific SNMP managers can access a particular SNMP agent, SNMP access is granted through communities. To control access, you first create an SNMP community. 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 has traps, which 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 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 J-series Services Router 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 router.
- Configure network interfaces. See the *J-series Services Router Basic LAN and WAN Access 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 5 shows the Quick Configuration page for SNMP.

Figure 5: Quick Configuration Page for SNMP

Juniper
NETWORKS

ROUTER - J2300

Monitor **Configuration** Diagnose Manage Events Alarms Logged in as: regress Help About Logout

Quick Configuration View and Edit History Rescue

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)

Copyright © 2004-2006, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

To configure SNMP features with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Quick Configuration > SNMP**.
2. Enter information into the Quick Configuration page for SNMP, as described in Table 22.
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 43.

Table 22: 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>J4300 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.

Table 22: SNMP Quick Configuration Summary (continued)

Field	Function	Your Action
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.
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 22: SNMP Quick Configuration Summary (continued)

Field	Function	Your Action
Enable Health Monitoring	<p>Enables the SNMP health monitor on the router. The health monitor periodically (the time you specify in the interval field) checks the following key indicators of router 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 the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

- Defining System Identification Information (Required) on page 39
- Configuring SNMP Agents and Communities (Required) on page 40
- Managing SNMP Trap Groups (Required) on page 41
- Controlling Access to MIBs (Optional) on page 42

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 23 identifies types of basic system identification and the MIB objects into which it is stored.

Table 23: 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 24.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 43.

Table 24: 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 Configuration > View and Edit > Edit Configuration. 2. Next to Snmp, click Configure or Edit. 	From the [edit] hierarchy level, enter edit snmp
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: set contact " <i>contact-information</i> "
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: set location " <i>location-information</i> "
Configure the system description (<i>J4300 with 4 PIMs</i> , for example).	In the Description box, type the description information as a free-form text string.	Set the description information: set description " <i>description-information</i> "
Configure a system name to override the system hostname defined in the Getting Started Guide for your router.	In the System Name box, type the system name as a free-form text string.	Set the system name: set name <i>name</i>
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: set engine-id use-mac-address

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 router, and, when applicable, a list of valid clients that can access the router.

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 25.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 43.

Table 25: 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 Configuration > View and Edit > Edit Configuration. 2. Next to Snmp, click Configure or Edit. 	From the [edit] hierarchy level, enter <code>edit snmp</code>
Create and name a community.	<ol style="list-style-type: none"> 1. Next to Community, click Add new entry. 2. In the Community box, type the name of the community as a free-form text string. 	Create a community: <code>set community community-name</code>
Grant read-write access to the community.	In the Authorization box, select read-write from the list.	Set the authorization to read-write: <code>set community community-name authorization read-write</code>
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"> 1. Next to Clients, click Add new entry. 2. In the Prefix box, type the IP address, in dotted decimal notation. 3. Click OK. 	Configure client access for the IP address 10.10.10.10: <code>set community community-name clients 10.10.10.10</code>
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"> 1. Next to Clients, click Add new entry. 2. In the Prefix box, type the IP address prefix 10.10.10.0/24, and click OK. 3. Next to Clients, click Add new entry. 4. In the Prefix box, type the IP address prefix 10.10.10.10/29. 5. Select the Restrict check box. 6. Click OK. 	<ol style="list-style-type: none"> 1. Configure client access for the IP address 10.10.10.0/24: <code>set community community-name clients 10.10.10.0/24</code> 2. Configure client access to restrict the IP addresses 10.10.10.10/29: <code>set community community-name clients 10.10.10.10/29 restrict</code>

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:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure SNMP trap groups, perform the configuration tasks described in Table 26.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 43.

Table 26: 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 Configuration > View and Edit > Edit Configuration. 2. Next to Snmp, click Configure or Edit. 	From the [edit] hierarchy level, enter <code>edit snmp</code>
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. 	Create a community: <code>set trap-group trap-group-name</code>
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. 	Set the trap-group target to 192.174.6.6: <code>set trap-group trap-group-name targets 192.174.6.6</code>
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. 	Configure the trap group categories: <code>set trap-group trap-group-name categories authentication chassis link</code>

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 27.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see “Verifying the SNMP Configuration” on page 43.

Table 27: 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 Configuration > View and Edit > Edit Configuration. 2. Next to Snmp, click Configure or Edit. 	From the [edit] hierarchy level, enter <code>edit snmp</code>
Create a view.	<ol style="list-style-type: none"> 1. Next to View, click Add new entry. 2. 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"> 1. Next to Oid, click Add new entry. 2. In the Name box, type the OID of the pingMIB, in either dotted integer or subtree name format. 3. 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"> 1. Next to Oid, click Add new entry. 2. In the Name box, type the OID of the jnxPingMIB, in either dotted integer or subtree name format. 3. 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"> 1. On the Snmp page, under Community, click the name of the community to which you want to apply the view. 2. In the View box, type the view name. 3. 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 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 </pre>
What It Means	<p>The output shows a list of the SNMP statistics, including details about the number and types of packets transmitted. Verify the following information:</p> <ul style="list-style-type: none"> ■ 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. <p>For more information about <code>show snmp statistics</code>, see the <i>JUNOS System Basics and Services Command Reference</i>.</p>

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 <code>show snmp health-monitor</code> command.
Sample Output	<pre> user@host> show snmp health-monitor </pre>

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)---
```

What It Means 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.

For more information about the `show snmp health-monitor` command, see the *JUNOS System Basics and Services Command Reference*.

Chapter 3

Configuring the Router as a DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP is particularly useful for managing a pool of IP addresses among hosts. 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 Services Router acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to router interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.



NOTE: Currently, the DHCP server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, or dynamic Domain Name System (DNS) updates. You cannot use DHCP for virtual private network (VPN) connections.

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

This chapter contains the following topics. For more information about DHCP, see the *JUNOS System Basics Configuration Guide*.

- DHCP Terms on page 47
- DHCP Overview on page 48
- Before You Begin on page 50
- Configuring the DHCP Server with Quick Configuration on page 50
- Configuring the DHCP Server with a Configuration Editor on page 56
- Verifying a DHCP Server Configuration on page 59

DHCP Terms

Before configuring the DHCP server on J-series Services Routers, become familiar with the terms defined in Table 28.

Table 28: 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 Services Router 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	Router 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: You cannot configure the Services Router as both a DHCP server and a BOOTP relay agent.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.

As a DHCP server, a Services Router can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. Services Routers 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 functions, you can also configure the Services Router to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Services Router).
- 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

Services Router 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.

Conflict Detection and Resolution

A client that receives an IP address from the Services Router 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 Services Router 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 Services Router supports DHCP client requests received on Fast Ethernet interfaces only. However, 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 Services Router 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 the DHCP Server with Quick Configuration

The DHCP Quick Configuration pages allow you to configure DHCP pools for subnets and static bindings for DHCP clients. If DHCP pools or static bindings are already configured, you can use the Configure Global DHCP Parameters Quick Configuration page to add settings for these pools and static bindings. Settings that have been previously configured for DHCP pools or static bindings are not overridden when you use the Configure Global DHCP Parameters Quick Configuration page.

Figure 6 through Figure 8 show the DHCP Quick Configuration pages.

Figure 6: DHCP Quick Configuration Main Page

Juniper
NETWORKS

ROUTER - J4300

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

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

Quick Configuration

DHCP

Global DHCP Parameters

Use the button below to configure global DHCP server parameters. These parameters will be inherited by any pools or static bindings that you set up. This option is useful if you have many pools or static bindings and wish to only specify this shared information once.

[Configure Global DHCP Parameters...](#)

DHCP Pools

DHCP is not configured to listen on any subnets.

[Add...](#)

DHCP Static Binding

DHCP is not configured to listen for any MAC addresses.

[Add...](#)

[OK](#) [Cancel](#) [Apply](#)

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) **Juniper your Net.**

Figure 7: DHCP Quick Configuration Pool Page

Juniper NETWORKS ROUTER - J4300

Monitor Configuration Diagnose Manage Events Logged in as: regress Help About Logout

Configuration > Quick Configuration > DHCP

Quick Configuration

DHCP [Add a DHCP Pool](#)

DHCP Pool Information

• DHCP Subnet

• Address Range (Low)

• Address Range (High)

Exclude Addresses

Lease Time

Maximum Lease Time (Seconds)

Default Lease Time (Seconds)

Server Information

Server Identifier

Domain Name

Domain Search

DNS Name Servers

Gateway Routers

WINS Servers

Boot Options

Boot File

Boot Server

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy Juniper your Net.

Figure 8: DHCP Quick Configuration Static Binding Page

Juniper NETWORKS **ROUTER - J4300**

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

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

Quick Configuration

DHCP **Add a DHCP Static Binding**

DHCP Static Binding Information

• DHCP MAC Address ?

• Fixed IP Address ?

?

Host Name ?

Client Identifier ?

Hexadecimal Client Identifier ?

Boot Options

Boot File ?

Boot Server ?

Server Information

Server Identifier ?

Domain Name ?

Domain Search ?

DNS Name Servers ?

Gateway Routers ?

WINS Servers ?

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. **Juniper Your Net.**

To configure the DHCP server with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > DHCP**.
2. Access a DHCP Quick Configuration page:
 - To configure a DHCP pool for a subnet, click **Add** in the DHCP Pools box.
 - To configure a static binding for a DHCP client, click **Add** in the DHCP Static Binding box.
 - To globally configure settings for existing DHCP pools and static bindings, click **Configure Global DHCP Parameters**.
3. Enter information into the DHCP Quick Configuration pages, as described in Table 29.
4. Click one of the following buttons on the DHCP Quick Configuration page:
 - To apply the configuration and return to the Quick Configuration page, click **OK**.
 - To cancel your entries and return to the Quick Configuration page, click **Cancel**.
5. Go on to one of the following procedures:
 - To display the configuration, see “Displaying a DHCP Server Configuration” on page 60.
 - To verify DHCP operation, see “Verifying a DHCP Server Configuration” on page 59.

Table 29: DHCP Server Quick Configuration Pages Summary

Field	Function	Your Action
DHCP Pool Information		
DHCP Subnet (required)	Specifies the 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 DHCP 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 DHCP Subnet. This address must be greater than the address specified in Address Range (Low).

Table 29: DHCP Server Quick Configuration Pages Summary (continued)

Field	Function	Your Action
Exclude Addresses	Specifies addresses to exclude from the IP address pool.	Do either 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.
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 4,294,967,295 (seconds). You can also type infinite to specify a lease that never expires.
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 2,147,483,647 (seconds). You can also type infinite to specify a lease that never expires.
Server Information		
Server Identifier	Specifies the IP address of the DHCP server reported to a client.	Type the IP address of the Services Router. 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 clients must use to resolve hostnames.	Type the name of the domain.
Domain Search	Specifies the order—from top to bottom—in which clients must append domain names when resolving hostnames using DNS.	Do either 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.
DNS Name Servers	Defines a list of DNS servers the client can use, in order of preference—from top to bottom.	Do either 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 DNS Name Servers box, and click Delete.
Gateway Routers	Defines a list of relay agents on the subnet, in order of preference—from top to bottom.	Do either 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.

Table 29: DHCP Server Quick Configuration Pages Summary (continued)

Field	Function	Your Action
WINS Servers	Defines a list of NetBIOS name servers, in order of preference—from top to bottom.	Do either 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.
Boot Options		
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Type a path and filename.
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.
DHCP Static Binding Information		
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.
Fixed IP Addresses (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 either of the following: <ul style="list-style-type: none"> ■ To add an IP address, type it next to the Add button, and click Add. ■ To remove an IP address, select it in the Fixed IP Addresses box, and click Delete.
Host Name	Specifies the name of the client used in 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.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in string form.
Hexadecimal Client Identifier	Specifies the name of the client, in hexadecimal, used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in hexadecimal form.

Configuring the DHCP Server with a Configuration Editor

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a Services Router 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 30 provides the settings and values for the sample DHCP server configuration used in this section.

Table 30: Sample DHCP Server 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
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 Services Router 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 31.
3. If you are finished configuring the router, commit the configuration.

4. To verify DHCP server configuration and operation, see “Verifying a DHCP Server Configuration” on page 59.

Table 31: Configuring the 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Configure or Edit. 3. Next to Services, make sure the check box is selected, and click Configure or Edit. 4. Next to Dhcp, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system services dhcp
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. 	Set the IP address pool range: set pool 192.168.2.0/24 address-range low 192.168.2.2 high 192.168.2.254
Define the default and maximum lease times, in seconds.	<ol style="list-style-type: none"> 1. From the Default lease time list, select Enter Specific Value. 2. In the Length box, type 1209600. 3. From the Maximum lease time list, select Enter Specific Value. 4. Next to Maximum lease time, type 2419200. 	Set the default and maximum lease times: set pool 192.168.2.0/24 default-lease-time 1209600 maximum-lease-time 2419200
Define the domain search suffixes to be used by the clients.	<ol style="list-style-type: none"> 1. Next to Domain search, click Add new entry. 2. In the Suffix box, type mycompany.net. 3. Click OK. 4. Next to Domain search, click Add new entry. 5. In the Suffix box, type mylab.net. 6. Click OK. 	Set the domain search suffixes: set pool 192.168.2.0/24 domain-search mycompany.net set pool 192.168.2.0/24 domain-search mylab.net

Table 31: Configuring the DHCP Server (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Exclude addresses from the IP address pool.	<ol style="list-style-type: none"> Next to Exclude address, click Add new entry. In the Address box, type 192.168.2.33. Click OK. 	Set the address to exclude from the IP address pool: <pre>set pool 192.168.2.0/24 exclude-address 192.168.2.33</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>

Verifying a DHCP Server Configuration

To verify a DHCP server configuration, perform the following tasks:

- Displaying a DHCP Server Configuration on page 60
- Verifying the DHCP Binding Database on page 60
- Verifying DHCP Server Operation on page 62
- Displaying DHCP Statistics on page 63

Displaying a DHCP Server Configuration

Purpose Verify the configuration of a DHCP server.

Action From the J-Web interface, select **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the `show system services dhcp` command from the top level.

You can also view the IP address pool from the CLI in operational mode by entering the `show system services dhcp pool` command.

Sample Output

```
[edit]
user@host# show system services dhcp
pool 192.168.2.0/24 {
    address-range low 192.168.2.2 high 192.168.2.254;
    exclude-address {
        192.168.2.33;
    }
    maximum-lease-time 2419200;
    default-lease-time 1209600;
    name-server {
        192.168.10.2;
    }
    domain-search {
        mycompany.net;
        mylab.net;
    }
    option 16 ip-address 192.168.2.33;
}
static-binding 01.03.05.07.09.0b {
    fixed-address {
        192.168.2.50;
    }
}
```

What It Means Verify that the output shows the intended configuration of the DHCP server. For more information about the format of a configuration file, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

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 all bindings in the database, including their current binding state, enter the `show system services dhcp binding detail` command. To display more information about a client, including its DHCP options, enter the `show system services dhcp binding ip-address detail` command, replacing *ip-address* with the IP address of the client.

The DHCP binding database resulting from the configuration defined in “Configuring the DHCP Server with a Configuration Editor” on page 56 is displayed in the following sample output.

To clear the DHCP binding database, enter the `clear system services dhcp binding` command. To remove a specific entry from the DHCP binding database, enter the `clear system services dhcp binding ip-address` command, replacing *ip-address* with the IP address of the client.

You can also use the J-Web interface to view information in the DHCP binding database. For more information, see “Monitoring DHCP” on page 118.

Sample Output

```
user@host> show system services dhcp binding

IP Address    Hardware Address  Type           Lease expires at
192.168.2.2   02:04:06:08:0A:0C dynamic        2005-02-07 8:48:59 PDT
192.168.2.50  01:03:05:07:09:0B static         never

user@host> show system services dhcp binding 192.168.2.2 detail

IP address          192.168.2.2
Hardware address     02:04:06:08:0A:0C
Pool                 192.168.2.0/24
Request received on fe-0/0/0

Lease information:
Type                DHCP
Obtained at         2005-01-24 8:48:59 PDT
Expires at          2005-02-07 8:48:59 PDT
State               active

DHCP options:
Name: domain-name, Value: mycompany.net mylab.net
Name: name-server, Value: 192.168.10.2
Code: 16, Type: ip-address, Value: 192.168.2.33

user@host> show system services dhcp conflict
```

What It Means

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 ip-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.

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 Services Router.
- 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
```

What It Means

Verify the following:

- The client returns a ping response.

For information about using the J-Web interface to ping a host, see “Using the J-Web Ping Host Tool” on page 204. For more information about the `ping` command, see “Pinging Hosts from the CLI” on page 223 or the *JUNOS System Basics and Services Command Reference*.

- The client IP configuration displayed contains the configured values. For example, for the DHCP configuration in “Configuring the DHCP Server with a Configuration Editor” on page 56, 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 Services Router 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 Services Router, including the client’s hostname, default gateways, and WINS servers.

Displaying DHCP Statistics

Purpose Display DHCP statistics, including lease times, packets dropped, and DHCP and BOOTP messages received and sent, to verify normal operation.

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

Sample Output

```
user@host> show system services dhcp statistics
```

```
Packets dropped:
  Total                      0
```

```
Messages received:
  BOOTREQUEST                0
  DHCPDECLINE                0
  DHCPDISCOVER               0
  DHCPINFORM                 0
  DHCPRELEASE                0
  DHCPREQUEST                78
```

```
Messages sent:
  BOOTREPLY                  0
  DHCPOFFER                  0
  DHCPACK                    78
  DHCPNAK                    0
```

What It Means

Verify the following:

- The default settings displayed are consistent with your DHCP server configuration.
- The number of dropped packets and errors is small.
- DHCPREQUEST messages have been received and DHCPACK messages have been sent.

Chapter 4

Automating Network Operations and Troubleshooting

J-series Services Routers support automation of network operations and troubleshooting tasks using commit scripts, operation scripts, and event policies. 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.

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

- Defining and Enforcing Configuration Rules with Commit Scripts on page 65
- Automating Network Management and Troubleshooting with Operation Scripts on page 68
- Running Self-Diagnostics with Event Policies on page 71

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 65
- Enabling Commit Scripts on page 66
- Disabling Commit Scripts on page 67

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 32.
5. If you are finished configuring the network, commit the configuration.

Table 32: 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 Configuration > View and Edit > Edit Configuration. 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 <code>edit system scripts commit</code>
Enable the commit script file—for example, <code>commit-script.xml</code> .	<ol style="list-style-type: none"> 1. Next to File, click Add new entry. 2. In the File name box, type <code>commit-script.xml</code>. 3. Click OK. 	Set the script file name: <code>set file commit-script.xml</code>

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 66. 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 68
- Enabling Operation Scripts on page 69
- Executing Operation Scripts on page 70
- Disabling Operation Scripts on page 70

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 71.

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 router 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 the JUNOS software, an operation script can ensure your router is configured to avoid or work around the problem.
- Change your router'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 33.
5. If you are finished configuring the network, commit the configuration.

Table 33: 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 Configuration > View and Edit > Edit Configuration. 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 <code>edit system scripts op</code>
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: <code>set file op-script.xml</code>

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 71.

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 .xsl
```

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 69. 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 .xsl
```

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 .xsl
```

2. Commit the configuration:

```
user@host# commit  
commit complete
```



NOTE: You can later reactivate the operation script using the `activate system scripts op filename .xsl` 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 71
- Configuring Event Policies on page 72

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.
- 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 68.

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 34.
3. If you are finished configuring the network, commit the configuration.

Table 34: 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 Configuration > View and Edit > Edit Configuration. 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. 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. 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/ .	<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. 	
Configuring Event Policy		

Table 34: Configuring Event Policies (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Policy level in the configuration hierarchy.	<ol style="list-style-type: none"> On the main Configuration page next to Event options, click Configure or Edit. Next to Policy, click Add new entry. 	From the [edit] hierarchy level, enter <code>edit event-options policy event1</code>
Enter the policy name—for example, <code>event1</code> .	In the Policy name box, type <code>event1</code> .	
Configure the event name—for example, <code>SNMP_TRAP_LINK_DOWN</code> . The <code>SNMP_TRAP_LINK_DOWN</code> event occurs when an interface that is monitored by SNMP becomes unavailable.	<ol style="list-style-type: none"> Next to Events, click Add new entry. In the Event box, type <code>SNMP_TRAP_LINK_DOWN</code>. Click OK. 	Set the event name: <code>set events SNMP_TRAP_LINK_DOWN</code>
Define the action to be taken when the configured event occurs. For example, configure the Services Router to do the following when the <code>SNMP_TRAP_LINK_DOWN</code> event occurs for the <code>t1-3/0/0</code> interface:	<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 <code>SNMP_TRAP_LINK_DOWN.interface-name</code>. In the To event attribute value box, type <code>t1-3/0/0</code>. Click OK. Next to Then, click Configure. Next to Execute commands, click Configure. In the Destination box, type <code>bsd2</code>. In the Output filename box, type <code>config.txt</code>. From the Output format list, select text. Next to Commands, click Add new entry. In the Command box, type <code>show interfaces t1-3/0/0</code>. Click OK. Next to Commands, click Add new entry. In the Command box, type <code>show configuration interfaces t1-3/0/0</code>. Click OK. 	<ol style="list-style-type: none"> Set the condition to execute the event policy only when the <code>SNMP_TRAP_LINK_DOWN</code> event occurs for the <code>t1-3/0/0</code> interface: <code>set attributes-match SNMP_TRAP_LINK_DOWN.interface-name equals t1-3/0/0</code> Enter <code>edit then execute-commands</code> Set the commands to be executed when the configured event occurs: <code>set commands show interfaces t1-3/0/0</code> <code>set commands show configuration interfaces t1-3/0/0</code> Set the name and format of the file in which the output of the executed commands is to be uploaded to a destination server: <code>set output-filename config.txt</code> <code>output-format text</code> Set the name of the server to which the file containing the command output is to be uploaded: <code>set destination bsd2</code>

NOTE: Do not include spaces, the slash, or the percent sign (%) in the filename.

Part 2

Monitoring a Services Router

- Monitoring the Router and Routing Operations on page 77
- Monitoring Events and Managing System Log Files on page 129
- Configuring and Monitoring Alarms on page 143

Chapter 5

Monitoring the Router and Routing Operations

J-series Services Routers support a suite of J-Web tools and CLI operational mode commands for monitoring system health and performance. Monitoring tools and commands display the current state of the router.

This chapter contains the following topics. 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*.

- Monitoring Terms on page 77
- Monitoring Overview on page 78
- Before You Begin on page 83
- Using the Monitoring Tools on page 83

Monitoring Terms

Before monitoring J-series Services Routers, become familiar with the terms defined in Table 35.

Table 35: J-series 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.

Monitoring Overview

Use the J-Web Monitor and Manage options to monitor a Services Router. J-Web results are displayed in the browser.

You can also monitor the router 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:

- Monitoring Tools Overview on page 78
- Filtering Command Output on page 82

Monitoring Tools Overview

J-Web monitoring tools consist of the options that appear when you select **Monitor** in the task bar. The Monitor options display diagnostic information about the Services Router.

Alternatively, you can enter `show` commands from the CLI to display the same information, and often greater detail. CLI `show` commands display the current configuration and information about interfaces, routing protocols, routing tables, routing policy filters, and the chassis. Use the CLI `clear` command to clear statistics and protocol database information.

Table 36 describes the function of each J-Web Monitor option and lists the corresponding CLI `show` commands.

Table 36: J-Web Monitor Options and CLI show Commands

Monitor Option	Function	Corresponding CLI Commands
System	Displays Services Router system properties, such as the system identification and uptime, users, and resource usage. For details, see “Monitoring System Properties” on page 84.	■ <code>show system uptime</code>
		■ <code>show system users</code>
		■ <code>show system storage</code>
		■ <code>show system processes</code>
Chassis	Displays alarm, environment, and hardware information. For details, see “Monitoring the Chassis” on page 87.	■ <code>show chassis alarms</code>
		■ <code>show chassis environment</code>
		■ <code>show chassis hardware</code>
Interfaces	Hierarchically displays all Services Router physical and logical interfaces, including state and configuration information. For details, see “Monitoring the Interfaces” on page 89.	■ <code>show interfaces terse</code>
		■ <code>show interfaces detail</code>
		■ <code>show interfaces interface-name</code>

Table 36: J-Web Monitor Options and CLI show Commands (continued)

Monitor Option	Function	Corresponding CLI Commands
Routing	<p>Displays routing information through the following options:</p> <ul style="list-style-type: none"> ■ Route Information—Information about the routes in a routing table, including destination, protocol, state, and parameter information. You can narrow the list of routes displayed by specifying search criteria. ■ OSPF Information—Summary of OSPF neighbors, interfaces, and statistics. ■ BGP Information—Summary of BGP routing and neighbor information. ■ RIP Information—Summary of RIP neighbors and statistics. ■ DLSw Information—Summary of DLSw circuits and peers. <p>For details, see “Monitoring Routing Information” on page 91.</p>	<ul style="list-style-type: none"> ■ Route information <ul style="list-style-type: none"> ■ show route terse ■ show route detail ■ OSPF information <ul style="list-style-type: none"> ■ show ospf neighbors ■ show ospf interfaces ■ show ospf statistics ■ BGP information <ul style="list-style-type: none"> ■ show bgp summary ■ show bgp neighbor ■ RIP information <ul style="list-style-type: none"> ■ show rip statistics ■ show rip neighbors ■ DLSw information <ul style="list-style-type: none"> ■ show dlsw capabilities ■ show dlsw circuits ■ show dlsw peers ■ show dlsw reachability

Table 36: J-Web Monitor Options and CLI show Commands (continued)

Monitor Option	Function	Corresponding CLI Commands
Class of Service (CoS)	<p>Displays information about the performance of class of service on a router through the following options:</p> <ul style="list-style-type: none"> ■ Interfaces—Displays the physical and logical interfaces in the system and provides details about the CoS components assigned to these interfaces. ■ Classifiers—Displays the forwarding classes and loss priorities that incoming packets are assigned to based on the packet's CoS values. ■ CoS Value Aliases—Displays the CoS value aliases that the system is using to represent Differentiated Services code point (DSCP), DSCP IPv6, MPLS experimental (EXP), and IPv4 precedence bits. ■ RED Drop Profiles—Displays detailed information about the drop profiles used by the system. Also, displays a graph of the random early detection (RED) curve that the system uses to determine the queue fullness and drop probability. ■ Forwarding Classes—Displays the assignment of forwarding classes to queue numbers. ■ Rewrite Rules—Displays packet CoS value rewrite rules based on the forwarding classes and loss priorities. ■ Scheduler Maps—Displays the assignment of forwarding classes to schedulers. Schedulers include transmit rate, rate limit, and buffer size. <p>For details, see “Monitoring Class-of-Service Performance” on page 98.</p>	<ul style="list-style-type: none"> ■ Interfaces—show class-of-service interface ■ Classifiers—show class-of-service classifier ■ CoS value aliases—show class-of-service code-point-aliases ■ RED drop profiles—show class-of-service drop-profile ■ Forwarding classes—show class-of-service forwarding-class ■ Rewrite rules—show class-of-service rewrite-rule ■ Scheduler maps—show class-of-service scheduler-map

Table 36: J-Web Monitor Options and CLI show Commands (continued)

Monitor Option	Function	Corresponding CLI Commands
MPLS	Displays information about MPLS label-switched paths (LSPs) and virtual private networks (VPNs) through the following options:	■ Interfaces— <code>show mpls interface</code>
	■ Interfaces—Information about the interfaces on which MPLS is enabled, including operational state and any administrative groups applied to an interface.	■ LSP information— <code>show mpls lsp</code>
	■ LSP Information—Information about LSP sessions currently active on the Services Router, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	■ LSP Statistics— <code>show mpls lsp statistics</code>
	■ LSP Statistics—Statistics for LSP sessions currently active on the Services Router, including the total number of packets and bytes forwarded through an LSP.	■ RSVP Sessions— <code>show rsvp session</code>
	■ RSVP Sessions—Information about RSVP-signaled LSP sessions currently active on the Services Router, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	■ RSVP Interfaces— <code>show rsvp interface</code>
	■ RSVP Interfaces—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.	
	For details, see “Monitoring MPLS Traffic Engineering Information” on page 106.	
Service Sets	Displays information about configured service sets.	■ <code>show services service-sets summary</code>
	For details, see “Monitoring Service Sets” on page 111.	■ <code>show services service-sets memory-usage</code>
Firewall	Displays firewall and intrusion detection service (IDS) information through the following options:	■ Stateful firewall information
	■ Stateful Firewall—Displays the stateful firewall configuration.	■ <code>show services stateful-firewall conversations</code>
	■ IDS Information—Displays information about the configured IDS.	■ <code>show services stateful-firewall flows</code>
	For details, see “Monitoring Firewalls” on page 112.	■ IDS information
		■ <code>show services ids destination-table</code>
		■ <code>show services ids source-table</code>
		■ <code>show services ids pair-table</code>

Table 36: J-Web Monitor Options and CLI show Commands (continued)

Monitor Option	Function	Corresponding CLI Commands
IPSec	Displays configured IPSec tunnels and statistics, and IKE security associations.	■ <code>show services ipsec-vpn ipsec statistics</code>
	For details, see “Monitoring IPSec Tunnels” on page 116.	■ <code>show services ipsec-vpn ipsec security-associations</code>
		■ <code>show services ipsec-vpn ike security-associations</code>
NAT	Displays configured NAT pools.	■ <code>show services nat pool</code>
	For details, see “Monitoring NAT Pools” on page 118.	
DHCP	Displays DHCP dynamic and static leases, conflicts, pools, and statistics.	■ <code>show system services dhcp binding</code>
	For details, see “Monitoring DHCP” on page 118.	■ <code>show system services dhcp conflict</code>
		■ <code>show system services dhcp pool</code>
		■ <code>show system services dhcp statistics</code>
RPM	Displays probe results for all RPM probes configured on the Services Router, including the round-trip times, jitter, and loss percentage of probes sent. Additionally, the RPM monitoring page displays a graph that plots the probe results as a function of time. For details, see “Monitoring RPM Probes” on page 120.	<code>show services rpm probe-results</code>
PPPoE	Displays the following PPPoE information:	■ <code>pppoe interfaces—show pppoe interfaces</code>
	■ PPPoE Interfaces—Session-specific information about the interfaces on which PPPoE is enabled.	■ <code>pppoe statistics—show pppoe statistics</code>
	■ PPPoE Statistics—Statistics for PPPoE sessions currently active.	■ <code>pppoe version—show pppoe version</code>
	■ PPPoE Version—Information about the PPPoE protocol currently configured on the router.	
	For details, see “Monitoring PPPoE” on page 124.	

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 Services Router 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 *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Before You Begin

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 14 and the *JUNOS System Basics Configuration Guide*.

Using the Monitoring Tools

This section describes the monitoring tools in detail. It contains the following topics:

- Monitoring System Properties on page 84
- Monitoring the Chassis on page 87
- Monitoring the Interfaces on page 89
- Monitoring Routing Information on page 91
- Monitoring Class-of-Service Performance on page 98
- Monitoring MPLS Traffic Engineering Information on page 106
- Monitoring Service Sets on page 111
- Monitoring Firewalls on page 112
- Monitoring IPSec Tunnels on page 116
- Monitoring NAT Pools on page 118
- Monitoring DHCP on page 118
- Monitoring RPM Probes on page 120
- Monitoring PPP on page 123
- Monitoring PPPoE on page 124

Monitoring System Properties

The system properties include everything from the name and IP address of the Services Router to the resource usage on the Routing Engine. To view these system properties, select **Monitor > System** in the J-Web interface, or enter the following CLI `show` commands:

- `show system uptime`
- `show system users`
- `show system storage`

Table 37 summarizes key output fields in system properties displays.

Table 37: Summary of Key System Properties Output Fields

Field	Values	Additional Information
System Identification		
Serial Number	Serial number for the J-series Services Router.	

Table 37: Summary of Key System Properties Output Fields (continued)

Field	Values	Additional Information
JUNOS Software Version	Version of JUNOS software active on the Services Router, including whether the software is for domestic or export use.	Export software is for use outside of the U.S. and Canada.
Router Hostname	Hostname of the Services Router, as defined with the set system hostname command.	
Router IP Address	IP address, in dotted decimal notation, of Ethernet management port 0 (fe-0/0/0 , for example), as defined with the set interfaces fe-0/0/0 command.	
Loopback Addresses	IP address, in dotted decimal notation, of the loopback address, as defined with the set interfaces lo0 command.	
Domain Name Servers	IP addresses, in dotted decimal notation, of the domain name servers, as defined with the set system name-server command.	
Time Zone	Time zone of the Services Router, as defined with the set system time-zone command.	
System Time		
Current Time	Current system time, in Coordinated Universal Time (UTC).	
System Booted Time	Date and time when the router was last booted and how long it has been running.	
Protocol Started Time	Date and time when the routing protocols were last started and how long they have been running.	
Last Configured Time	Date and time when a configuration was last committed. This field also shows the name of the user who issued the last commit command, through either the J-Web interface or the CLI.	
Users		
User	Username of any user logged in to the Services Router.	
TTY	Terminal through which the user is logged in.	
From	System from which the user has logged in. A hyphen indicates that the user is logged in through the console.	
Login Time	Time when the user logged in.	This is the LOGIN@ field in show system users command output.
Idle Time	How long the user has been idle.	
Command	Processes that the user is running.	This is the WHAT field in show system users command output.
Memory Usage		

Table 37: Summary of Key System Properties Output Fields (continued)

Field	Values	Additional Information
Total Memory Available	Total RAM available on the Services Router.	
Total Memory Used	Total RAM currently being consumed by processes actively running on the Services Router, displayed both as a quantity of memory and as a percentage of the total RAM on the router.	
Process ID	Process identifier.	This is the PID field in <code>show system processes</code> command output.
Process Owner	Name of the process owner.	
Process Name	Command that is currently running.	Individual processes on the Services Router are listed here. Because each process within JUNOS operates in a protected memory environment, you can diagnose whether a particular process is consuming abnormally high amounts of resources. If a software process is using too much CPU or memory, you can restart the process by entering the <code>restart</code> command from the CLI.
CPU Usage	Percentage of the CPU that is being used by the process.	
Memory Usage	Percentage of the installed RAM that is being used by the process.	
CPU Usage		
Total CPU Used	Sum of CPU usages by all processes, expressed as a percentage of total CPU available.	
Process ID	Process identifier.	This is the PID field in <code>show system processes</code> command output.
Process Owner	Name of the process' owner.	
Process Name	Command that is currently running.	Individual processes on the Services Router are listed here. Because each process within JUNOS operates in a protected memory environment, you can diagnose whether a particular process is consuming an abnormal amount of resources. If a software process is using too much CPU or memory, you can restart the process by entering the <code>restart</code> command from the CLI.
CPU Usage	Percentage of the CPU that is being used by the process.	
Memory Usage	Percentage of the installed RAM that is being used by the process.	
System Storage		
Total Flash Size	Total size, in megabytes, of the primary flash device.	

Table 37: Summary of Key System Properties Output Fields (continued)

Field	Values	Additional Information
Usable Flash Size	Total usable memory, in megabytes, of the primary flash device.	The total usable flash memory is the total memory minus the size of the JUNOS image installed on the Services Router.
Flash Used	Total flash memory used, in megabytes and as a percentage of the total usable flash size, of the primary flash device.	
Log Files	Total size, in kilobytes, of the log files on the Services Router.	This is the sum of file sizes in the <code>/var/log</code> directory.
Temporary Files	Total size, in kilobytes, of the temporary files on the Services Router.	This is the sum of the file sizes in the <code>/var/tmp</code> directory.
Crash (Core) Files	Total size, in kilobytes, of the core files on the Services Router.	This is the sum of the file sizes in the <code>/var/crash</code> directory.
Database Files	Total size, in kilobytes, of the configuration database files on the Services Router.	This is the sum of the file sizes in the <code>/var/db</code> directory.

Monitoring System Process Information

To view the software processes running on the router, select **Monitor > System > Process Information** in the J-Web interface, or enter the CLI `show system processes` commands.

Table 38 summarizes the output fields in the system process information display.

Table 38: Summary of System Process Information Output Fields

Field	Values	Additional Information
Process ID	Identifier of the process.	
Effective User	Owner of the process.	
Command	Command that is currently running.	
Terminal	Terminal that is currently running.	
Status	Current status of the process.	
Sleep state	Sleep state of the process.	
Start time	Time of day when the process started.	

Monitoring the Chassis

The chassis properties include the status of any alarms on the Services Router, environment measurements, and a summary of the field-replaceable units (FRUs)

on the router. To view these chassis properties, select **Monitor > Chassis** in the J-Web interface, or enter the following CLI **show** commands:

- `show chassis alarms`
- `show chassis environment`
- `show chassis hardware`

Table 39 summarizes key output fields in chassis displays.

Table 39: Summary of Key Chassis Output Fields

Field	Values	Additional Information
Alarm Summary		
Alarm Time	Date and time the alarm was first recorded.	
Alarm Class	Severity class for this alarm: Minor or Major .	<p>JUNOS has system-defined alarms and configurable alarms. System-defined alarms include FRU detection alarms (power supplies removed, for instance) and environmental alarms. The values for these alarms are defined within JUNOS.</p> <p>Configurable alarms are set in either of the following ways:</p> <ul style="list-style-type: none">■ In the J-Web configuration editor, on the Chassis > Alarm > <i>interface-type</i> page■ In the CLI configuration editor, with the alarm statement at the [edit chassis] level of the configuration hierarchy <p>For details, see “Configuring and Monitoring Alarms” on page 143.</p>
Alarm Description	A brief synopsis of the alarm.	
Environment Information		
Name	Chassis component. For J-series Services Routers, the chassis components are the Routing Engine and the fan.	
Gauge Status	Status of the temperature gauge on the specified hardware component.	
Temperature	Temperature of the air flowing past the hardware component.	
Hardware Summary		
Name	Chassis component. For J-series Services Routers, the chassis components are the Routing Engine, the Physical Interface Module (PIM) slot number (identified in the display as an FPC), and the PIM number (identified in the display as a PIC).	On J-series Services Routers, an FPC and a PIM are the same physical unit. The PIM number is always 0.

Table 39: Summary of Key Chassis Output Fields (continued)

Field	Values	Additional Information
Version	Revision level of the specified hardware component.	Supply the version number when reporting any hardware problems to customer support.
Part Number	Part number of the chassis component.	
Serial Number	Serial number of the chassis component. The serial number of the backplane is also the serial number of the router chassis.	Use this serial number when you need to contact customer support about the router chassis.
Description	Brief description of the hardware item.	For J-series PIMs, the description lists the number and type of the ports on the PIM—identified in the display as a PIC.

Monitoring the Interfaces

The interface information is divided into multiple parts. To view general interface information such as available interfaces, operation states of the interfaces, and descriptions of the configured interfaces, select **Monitor > Interfaces** in the J-Web interface. To view interface-specific properties such as administrative state or traffic statistics in the J-Web interface, select the interface name on the Interfaces page.

Alternatively, enter the following CLI `show` commands:

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

Table 40 summarizes key output fields in interfaces displays.

Table 40: Summary of Key Interfaces Output Fields

Field	Values	Additional Information
Interface Summary		
Interface Name	Name of interface.	Click an interface name to see more information about the interface.
Oper State	Link state of the interface: Up or Down .	The operational state is the physical state of the interface. If the interface is physically operational, even if it is not configured, the operational state is Up . An operational state of Down indicates a problem with the physical interface.

Table 40: Summary of Key Interfaces Output Fields (continued)

Field	Values	Additional Information
Admin State	Whether the interface is enabled up (Up) or disabled (Down).	<p>Interfaces are enabled by default. To disable an interface:</p> <ul style="list-style-type: none"> ■ In the J-Web configuration editor, select the Disable check box on the Interfaces > interfaces-name page. ■ In the CLI configuration editor, add the disable statement at the [edit interfaces <i>interfaces-name</i>] level of the configuration hierarchy
Description	Configured description for the interface.	
Interface: <i>interface-name</i>		
State	Link state of the interface: Up or Down.	The operational state is the physical state of the interface. If the interface is physically operational, even if it is not configured, the operational state is Up. An operational state of Down indicates a problem with the physical interface.
Admin State	Whether the interface is enabled up (Up) or disabled (Down).	<p>Interfaces are enabled by default. To disable an interface:</p> <ul style="list-style-type: none"> ■ In the J-Web configuration editor, select the Disable check box on the Interfaces > interfaces-name page. ■ In the CLI configuration editor, add the disable statement at the [edit interfaces <i>interfaces-name</i>] level of the configuration hierarchy
MTU	Maximum transmission unit (MTU) size on the physical interface.	
Speed	Speed at which the interface is running.	
Current Address	Configured media access control (MAC) address.	
Hardware Address	Hardware MAC address.	
Last Flapped	Date, time, and how long ago the interface changed state from Down to Up.	
Active Alarms	List of any active alarms on the interface.	<p>Configure alarms on interfaces as follows:</p> <ul style="list-style-type: none"> ■ In the J-Web configuration editor, on the Chassis > Alarm > interface-type page ■ In the CLI configuration editor, with the alarm statement at the [edit chassis] level of the configuration hierarchy
Traffic Statistics	Number of packets and bytes received and transmitted on the physical interface.	

Table 40: Summary of Key Interfaces Output Fields (continued)

Field	Values	Additional Information
Input Errors	Input errors on the interface. (See the following rows of this table for specific error types.)	
Drops	Number of packets dropped by the output queue.	If the interface is saturated, this number increments once for every packet that is dropped by the Services Router's random early detection (RED) mechanism.
Framing errors	Sum of ATM Adaptation Layer (AAL5) packets that have frame check sequence (FCS) errors, AAL5 packets that have reassembly timeout errors, and AAL5 packets that have length errors.	
Policed discards	Number of packets dropped as a result of routing policies configured on the interface.	

Monitoring Routing Information

The J-Web interface provides information about routing tables and routing protocols.

This section contains the following topics:

- Monitoring Routing Information on page 91
- Monitoring BGP Routing Information on page 93
- Monitoring OSPF Routing Information on page 94
- Monitoring RIP Routing Information on page 96
- Monitoring DLSw Routing Information on page 97

Monitoring Routing Information

Routing information is divided into multiple parts:

- To view the inet.0 (IPv4) routing table in the J-Web interface, select **Monitor > Routing > Route Information**, or enter the following CLI commands:
 - `show route terse`
 - `show route detail`

Table 41 summarizes key output fields in the routing information display.

Table 41: 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 Services Router. 	
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 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 Routing Protocols and Policies 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 BGP Routing Information

To view BGP routing information, select **Monitor > Routing > BGP Information**, or enter the following CLI commands:

- `show bgp summary`
- `show bgp neighbor`

Table 42 summarizes key output fields in the BGP routing display.

Table 42: 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.
State	A multipurpose field that displays information about BGP peer sessions. The contents of this field depend upon whether a session is established. <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 .	

Table 42: Summary of Key BGP Routing Output Fields (continued)

Field	Values	Additional Information
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 OSPF Routing Information

To view OSPF routing information, select **Monitor > Routing > OSPF Information**, or enter the following CLI commands:

- `show ospf neighbors`
- `show ospf interfaces`
- `show ospf statistics`

Table 43 summarizes key output fields in the OSPF routing display.

Table 43: 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 43: 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 RIP Routing Information

To view RIP routing information, select **Monitor > Routing > RIP Information**, or enter the following CLI commands:

- show rip statistics
- show rip neighbors

Table 44 summarizes key output fields in the RIP routing display.

Table 44: 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.	<p>This value is the name of the interface on which RIP is enabled. The name is set in either of the following ways:</p> <ul style="list-style-type: none"> ■ In the J-Web configuration editor, on the Protocols > RIP > Group > group-name > Neighbor page ■ In the CLI configuration editor, with the <code>neighbor neighbor-name</code> statement at the <code>[edit protocols rip group group-name]</code> level of the configuration hierarchy

Table 44: Summary of Key RIP Routing Output Fields (continued)

Field	Values	Additional Information
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 DLSw Routing Information

To view DLSw routing information, select **Monitor > Routing > DLSw Information**, or enter the following CLI commands:

- show dlsw capabilities
- show dlsw circuits
- show dlsw peers
- show dlsw reachability

Table 45 summarizes key routing information output fields in the DLSw routing display.

Table 45: Summary of Key DLSw Routing Information Output Fields

Field	Values	Additional Information
DLSw Capabilities		
Peer	IP address of the peer DLSw router	
Vendor ID	Numerical value assigned to Juniper Networks.	
Version number	DLSw protocol version.	
Initial pacing window	Frequency at which packets are sent.	
Version string	Juniper Networks software version information.	
DLSw Circuits		
Circuit id	DLSw circuit ID	
Local Address	MAC address of the local DLSw peer.	
LSAP	Number of the local service access point.	

Table 45: Summary of Key DLSw Routing Information Output Fields (continued)

Field	Values	Additional Information
Remote address	MAC address of the remote DLSw peer.	
DSAP	Number of the destination service access point.	
State (or circuit state)	Connectivity status; disconnected or connected.	
Peer (or remote peer address)	IP address of the remote DLSw peer.	
DLSw Peers		
Peer	IP address of the remote DLSw peer.	
State	Status of the connection.	
Circuits	Number of circuits on the DLSw network.	
Local address	IP address of the local DLSw peer.	
Created time	Time of circuit creation.	
Connected time	Length of time that the connection is active.	
Receive initial pacing	Size of the initial pacing frame.	
No circuits timeout	Length of time before a circuit becomes inactive.	
DLSw Reachability		
MAC index	Number assigned to the remote DLSw peer.	
MAC address	MAC address of the remote DLSw peer.	
Remote DLSw address	IP address of the remote DLSw peer.	

Monitoring Class-of-Service Performance

The J-Web interface provides information about the class-of-service (CoS) performance on a router. 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 99
- Monitoring CoS Classifiers on page 100
- Monitoring CoS Value Aliases on page 101
- Monitoring CoS RED Drop Profiles on page 101
- Monitoring CoS Forwarding Classes on page 102
- Monitoring CoS Rewrite Rules on page 103
- Monitoring CoS Scheduler Maps on page 104

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 46 summarizes key output fields for CoS interfaces.

Table 46: Summary of Key CoS Interfaces Output Fields

Field	Values	Additional Information
Interface	Name of a physical interface to which CoS components are assigned.	To display names of logical interfaces configured on this physical interface, click the plus sign (+).
Scheduler Map	Name of the scheduler map associated with this interface.	
Queues Supported	Number of queues you can configure on the interface.	
Queues in Use	Number of queues currently configured.	
Logical Interface	Name of a logical interface on the physical interface, to which CoS components are assigned.	
Object	Category of an object—for example, classifier, scheduler-map, or rewrite.	
Name	Name that you have given to an object—for example, ba-classifier.	

Table 46: Summary of Key CoS Interfaces Output Fields (continued)

Field	Values	Additional Information
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 47 summarizes key output fields for CoS classifiers.

Table 47: 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.	
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 router.	
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 48 summarizes key output fields for CoS value aliases.

Table 48: 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 49 summarizes key output fields for CoS RED drop profiles.

Table 49: 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 50 summarizes key output fields for CoS forwarding classes.

Table 50: 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 51 summarizes key output fields for CoS rewrite rules.

Table 51: Summary of Key CoS Rewrite Rules Output Fields

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	

Table 51: Summary of Key CoS Rewrite Rules Output Fields (continued)

Field	Values	Additional Information
CoS Value Type	Rewrite rule type: <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.	
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 52 summarizes key output fields for CoS scheduler maps.

Table 52: 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.	

Table 52: Summary of Key CoS Scheduler Maps Output Fields (continued)

Field	Values	Additional Information
Transmit Rate	<p>Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following:</p> <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	<p>Rate limiting configuration of the queue:</p> <ul style="list-style-type: none"> ■ none—No rate limiting. ■ exact—The queue transmits at only the configured rate. 	
Buffer Size	<p>Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following:</p> <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	<p>Scheduling priority of a queue:</p> <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.	

Table 52: Summary of Key CoS Scheduler Maps Output Fields (continued)

Field	Values	Additional Information
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 Multiprotocol Label Switching (MPLS) traffic engineering.

This section contains the following topics:

- Monitoring MPLS Interfaces on page 106
- Monitoring MPLS LSP Information on page 107
- Monitoring MPLS LSP Statistics on page 108
- Monitoring RSVP Session Information on page 109
- Monitoring MPLS RSVP Interfaces Information on page 110

Monitoring MPLS Interfaces

To view the interfaces on which MPLS is configured, select **Monitor > MPLS > Interfaces**, or enter the following CLI command:

```
show mpls interface
```

Table 53 summarizes key output fields in the MPLS interface information display.

Table 53: 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 54 summarizes key output fields in the MPLS LSP information display.

Table 54: Summary of Key MPLS LSP Information Output Fields

Field	Values	Additional Information
Ingress LSP	Information about LSPs on the inbound router. Each session has one line of output.	
Egress LSP	Information about the LSPs on the outbound router. 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 router) of the session.	
From	Source (inbound router) 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.	

Table 54: Summary of Key MPLS LSP Information Output Fields (continued)

Field	Values	Additional Information
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 accounting information about LSPs, 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 router, because the penultimate router in the LSP sets the label to 0. Also, as the packet arrives at the outbound router, 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 55 summarizes key output fields in the MPLS LSP statistics display.

Table 55: Summary of Key MPLS LSP Statistics Output Fields

Field	Values	Additional Information
Ingress LSP	Information about LSPs on the inbound router. Each session has one line of output.	
Egress LSP	Information about the LSPs on the outbound router. 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 router) of the session.	
From	Source (inbound router) of the session.	
State	State of the path: Up , Down , or AdminDn .	AdminDn indicates that the LSP is being taken down gracefully.

Table 55: Summary of Key MPLS LSP Statistics Output Fields (continued)

Field	Values	Additional Information
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 currently active RSVP session information, select **Monitor > MPLS > RSVP Sessions**, or enter the following CLI command:

```
show rsvp session
```

Table 56 summarizes key output fields in the RSVP session information display.

Table 56: Summary of Key RSVP Session Information Output Fields

Field	Values	Additional Information
Ingress LSP	Information about inbound RSVP sessions. Each session has one line of output.	
Egress LSP	Information about outbound RSVP sessions. Each session has one line of output.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
Transit LSP	Information about transit RSVP sessions.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
To	Destination (outbound router) of the session.	
From	Source (inbound router) 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.	

Table 56: Summary of Key RSVP Session Information Output Fields (continued)

Field	Values	Additional Information
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 the interfaces on which RSVP is running, select **Monitor > MPLS > RSVP Interfaces**, or enter the following CLI command:

```
show rsvp interface
```

Table 57 summarizes key output fields in the RSVP interfaces information display.

Table 57: Summary of Key RSVP Interfaces Information Output Fields

Field	Values	Additional Information
RSVP Interface	Number of interfaces on which RSVP is active. Each interface has one line of output.	
Interface	Name of the interface.	
State	State of the interface: <ul style="list-style-type: none"> ■ 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).	

Table 57: Summary of Key RSVP Interfaces Information Output Fields (continued)

Field	Values	Additional Information
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 Service Sets

A service set is a group of rules from a stateful firewall filter, Network Address Translation (NAT), intrusion detection service (IDS), or IP Security (IPSec) that you apply to a services interface. You can configure IDS, NAT, and stateful firewall filter service rules within the same service set. You must configure IPSec services in a separate service set. For more information about using service sets with these features, see the *J-series Services Router Advanced WAN Access Configuration Guide*.

Service set information includes the services interfaces on the Services Router, the number of services sets configured on the interfaces, and the total CPU used by the service sets. To view these service set properties, select **Monitor > Service Sets** in the J-Web interface, or enter the following CLI `show` commands:

- `show services service-sets summary`
- `show services service-sets memory-usage`

Table 58 summarizes key output fields in service sets displays.

Table 58: Summary of Key Service Set Output Fields

Field	Values	Additional Information
Service Set Summary		
Interface	Name of the adaptive services interface on the Services Router—always <code>sp-0/0/0</code> .	
Service sets configured	Total number of service sets configured on the Services Router.	
Bytes used	Total number of general-purpose memory bytes being used by the service set configuration.	A portion of the general-purpose memory on a Services Router is allocated for storing traffic flows, NAT pools, and so on.
Policy bytes used	Total number of configuration-object memory bytes being used by routing policies associated with the service set configuration.	A portion of the general-purpose memory on a Services Router is allocated for storing configuration objects like firewall rules, routing policies, and so on.
CPU utilization	Percentage of the CPU resources being used.	A high CPU utilization indicates that the router is under heavy load. High CPU utilization might cause performance degradation in forwarding or the application of other services.
Memory Usage		

Table 58: Summary of Key Service Set Output Fields (continued)

Field	Values	Additional Information
Interface	Name of the adaptive services interface on the Services Router—always sp-0/0/0 .	
Service set	Name of a service set.	
Memory Utilization %	Percentage of the memory resources being used by the service set.	A high CPU utilization indicates that the router is under heavy load. High CPU utilization might cause performance degradation in forwarding or the application of other services.
Memory zone	Memory zone in which the services interface is currently operating. Following are valid zones: <ul style="list-style-type: none"> ■ Green—All new flows are allowed. ■ Yellow—Unused memory is reclaimed. All new flows are allowed. ■ Orange—New flows are only allowed for service sets that are using less than their equal share of memory. ■ Red—No new flows are allowed. 	

Monitoring Firewalls

The firewall filter information is divided into three parts—firewall statistics, stateful firewall filters and intrusion detection services.

This section contains the following topics:

- Monitoring Stateful Firewall Statistics on page 112
- Monitoring Stateful Firewall Filters on page 114
- Monitoring Firewall Intrusion Detection Services (IDS) on page 114

Monitoring Stateful Firewall Statistics

To view stateful firewall filter statistics in the J-Web interface, select **Monitor > Firewall > Statistics Summary**. Alternatively, enter the CLI command `show services stateful-firewall statistics`.

Table 59 summarizes key output fields for stateful firewall filter statistics.

Table 59: Summary of Key Stateful Firewall Statistics Output Fields

Field	Values
Interface	Name of the services interface on which the service set is applied.
Service Set	Name of the service set.
Accept	Number of packets accepted by all rules defined in the service set.
Discard	Number of packets discarded by all rules defined in the service set.
Reject	Number of packets rejected by all rules defined in the service set.
New flows	<p>Number of packets matching rules defined in new flows:</p> <ul style="list-style-type: none"> ■ Accept—Number of packets accepted. ■ Discards—Number of packets discarded. ■ Rejects—Number of packets rejected.
Existing flows	<p>Number of packets matching rules defined in existing flows:</p> <ul style="list-style-type: none"> ■ Accept—Number of packets accepted. ■ Discards—Number of packets discarded. ■ Rejects—Number of packets rejected.
Drops	<p>Number of packets dropped due to the following match conditions:</p> <ul style="list-style-type: none"> ■ IP Option—Number of packets dropped due to the inspection of the IP options field of the packet. ■ TCP SYN Defense—Number of packets dropped due to the SYN defender, which prevents denial-of-service (DoS) attacks. ■ NAT Ports Exhausted—Number of packets dropped because the router has no available NAT ports to assign for a given source address. <p>For more information about these match conditions, see the <i>J-series Services Router Advanced WAN Access Configuration Guide</i> and the <i>JUNOS Services Interfaces Configuration Guide</i>.</p>
Errors	<p>Number of protocol errors detected:</p> <ul style="list-style-type: none"> ■ IP—Number of IPv4 errors (for example, Minimum IP header length check failures). ■ TCP—Number of TCP errors (for example, Source or destination port number is zero). ■ UDP—Number of UDP errors (for example, IP data length less than minimum UDP header length (8 bytes)). ■ ICMP—Number of ICMP errors (for example, Duplicate ping sequence number). ■ Non-IP Packets—Number of errors in packets that are not IPv4 packets. ■ ALG—Number of application-level gateway (ALG) errors. <p>For a complete list of protocol errors that are counted, see the description of the show services stateful-firewall statistics command in the <i>JUNOS System Basics and Services Command Reference</i>.</p>

Monitoring Stateful Firewall Filters

To view stateful firewall filter information in the J-Web interface, select **Monitor > Firewall > Stateful Firewall**. To display stateful firewall filter information for a particular address prefix, port, or other characteristic, type or select information in one or more of the Narrow Search boxes, and click **OK**.

Alternatively, enter the following CLI show commands:

- `show services stateful-firewall conversations`
- `show services stateful-firewall flows`

Table 60 summarizes key output fields for stateful firewall filters.

Table 60: Summary of Key Stateful Firewall Filters Output Fields

Field	Values
Protocol	Protocol used for the specified stateful firewall flow.
Source IP	Source prefix of the stateful firewall flow.
Source Port	Source port number of stateful firewall flow.
Destination IP	Destination prefix of the stateful firewall flow.
Destination Port	Destination port number of the stateful firewall flow.
Flow State	Status of the stateful firewall flow: <ul style="list-style-type: none"> ■ Drop—Drop all packets in the flow without response. ■ Forward—Forward the packet in the flow without inspecting it. ■ Reject—Drop all packets in the flow with response. ■ Watch—Inspect packets in the flow.
Direction	Direction of the flow: I (input) or O (output).
Frames	Number of frames in the flow.

Monitoring Firewall Intrusion Detection Services (IDS)

To view intrusion detection service (IDS) information for stateful firewall filters, select **Monitor > Firewall > IDS Information**. Click one of the following criteria to order the display accordingly:

- **Bytes** (received bytes)
- **Packets** (received packets)
- **Flows**
- **Anomalies**

To limit the display of IDS information, type or select information in one or more of the Narrow Search boxes listed in Table 61, and click **OK**.

Table 61: IDS Search-Narrowing Characteristics

Narrow Search Box	Entry or Selection
Destination Address	Type a destination address prefix to display IDS information for only that prefix.
IDS Table	Select one of the following: <ul style="list-style-type: none"> ■ Destination—Displays information for an address under attack. ■ Pair—Displays information for a suspected attack source and destination pair. ■ Source—Displays information for an address that is a suspected attacker.
Number of IDS Entries to Display	Select a number between 25 and 500 to display only a particular number of entries.
Threshold	Type a number to display events with only that number of bytes, packets, flows, or anomalies—whichever you selected to order the display. For example, to display all events with more than 100 flows, click Flows and then type 100 in the Threshold box.
Service Set	Select a service set to display information for only the set.

Alternatively, enter the following CLI **show** commands:

- `show services ids destination-table`
- `show services ids source-table`
- `show services ids pair-table`

Table 62 summarizes key output fields for stateful firewall filter intrusion detection.

Table 62: Summary of Key Firewall IDS Output Fields

Field	Values
Source Address	Source address for the event.
Destination address	Destination address for the event.
Time	Total time the information has been in the IDS table.
Bytes	Total number of bytes sent from the source to the destination address, in thousands (k) or millions (m).
Packets	Total number of packets sent from the source to the destination address, in thousands (k) or millions (m).
Flows	Total number of flows of packets sent from the source to the destination address, in thousands (k) or millions (m).

Table 62: Summary of Key Firewall IDS Output Fields (continued)

Field	Values
Anomalies	Total number of anomalies in the anomaly table, in thousands (k) or millions (m).
Application	Configured application, such as FTP or Telnet.

Monitoring IPSec Tunnels

IPSec tunnel information includes information about active IPSec tunnels configured on the Services Router, as well as traffic statistics through the tunnels. To view IPSec tunnel information, select **Monitor > IPSec** in the J-Web interface, or enter the following CLI **show** commands:

- `show services ipsec-vpn ipsec statistics`
- `show services ipsec-vpn ipsec security-associations`
- `show services ipsec-vpn ike security-associations`

Table 63 summarizes key output fields in IPSec displays.

Table 63: Summary of Key IPSec Output Fields

Field	Values
IPSec Tunnels	
Service Set	Name of the service set for which the IPSec tunnel is defined.
Rule	Name of the rule set applied to the IPSec tunnel.
Term	Name of the IPSec term applied to the IPSec tunnel.
Local Gateway	Gateway address of the local system.
Remote Gateway	Gateway address of the remote system.
Direction	Direction of the IPSec tunnel: Inbound or Outbound .
Protocol	Protocol supported: either Encapsulation Security Protocol (ESP) or Authentication Header and ESP (AH+ESP).
Tunnel Index	Numeric identifier of the IPSec tunnel.
Tunnel Local Identity	Prefix and port number of the local endpoint of the IPSec tunnel.
Tunnel Remote Identity	Prefix and port number of the remote endpoint of the IPSec tunnel.
IPSec Statistics	
Service Set	Name of the service set for which the IPSec tunnel is defined.
Local Gateway	Gateway address of the local system.
Remote Gateway	Gateway address of the remote system.
ESP Encrypted Bytes	Total number of bytes encrypted by the local system across the IPSec tunnel.

Table 63: Summary of Key IPSec Output Fields (continued)

Field	Values
ESP Decrypted Bytes	Total number of bytes decrypted by the local system across the IPSec tunnel.
AH Input Bytes	Total number of bytes received by the local system across the IPSec tunnel.
AH Output Bytes	Total number of bytes transmitted by the local system across the IPSec tunnel.
IKE Security	
Remote Address	Responder's address.
State	State of the IKE security association: <ul style="list-style-type: none"> ■ Matured—IKE security association is established. ■ Not matured—IKE security association is in the process of negotiation.
Initiator Cookie	Random number sent to the remote node when the IKE negotiation is triggered. This number is generated by means of an algorithm and information shared during the IKE negotiation. Cookies provide a basic form of authenticity protection to help prevent denial-of-service (DoS) attacks.
Responder Cookie	Random number generated by the remote node when it receives the initiator cookie. The remote node sends the cookie back to the IKE initiator as verification that the negotiation packets were received.
Exchange Type	Type of IKE exchange. The IKE exchange type determines the number of messages in the exchange and the payload types contained in each message. Each exchange type provides a particular set of security services, such as anonymity of the participants, perfect forward secrecy of the keying material, and authentication of the participants. J-series Services Routers support the following types of IKE exchanges: <ul style="list-style-type: none"> ■ Main—IKE exchange is done with six messages. The Main exchange type encrypts the payload, protecting the identity of the neighbor. ■ Aggressive—IKE exchange is done with three messages. The Aggressive exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected.
Role	Role of the router in the IKE exchange: Initiator or Responder .
Authentication Method	Method used for IKE authentication. The type of authentication determines which payloads are exchanged and when they are exchanged. J-series Services Routers support only the pre-shared keys authentication type.
Local Address	Prefix and port number of the local tunnel endpoint.
Remote Address	Prefix and port number of the remote tunnel endpoint.
Lifetime	Number of seconds remaining until the IKE security association expires.
Algorithm Authentication	Type of authentication algorithm used for the security association: md5 or sha1 .
Algorithm Encryption	Type of encryption algorithm used for the security association: des-cbc , 3des-cbc , or None .
Algorithm PRF	The pseudorandom function that generates highly unpredictable random numbers: hmac-md5 or hmac-sha1 .
Input Bytes	Number of bytes received on the IKE security association.
Output Bytes	Number of bytes transmitted on the IKE security association.
Input Packets	Number of packets received on the IKE security association.
Output Packets	Number of packets transmitted on the IKE security association.

Table 63: Summary of Key IPSec Output Fields (continued)

Field	Values
IPSec Security Associations	Number of IPSec security associations that have been created and deleted on the router. Only security associations whose negotiations are complete are listed. When a security association is taken down, it is listed as a deleted security association.
Phase 2 Negotiations in Progress	Number of phase 2 IKE negotiations in progress.

Monitoring NAT Pools

NAT pool information includes information about the address ranges configured within the pool on the Services Router. To view NAT pool information, select **Monitor > NAT** in the J-Web interface, or enter the following CLI show command:

```
show services nat pool
```

Table 64 summarizes key output fields in NAT displays.

Table 64: Summary of Key NAT Output Fields

Field	Values
NAT Pools	
NAT Pool	Name of the NAT pool.
Pool Start Address	Lower address in the NAT pool address range.
Pool Address End	Upper address in the NAT pool address range.
Port High	Upper port in the NAT pool port range.
Port Low	Lower port in the NAT pool port range.
Ports In Use	Number of ports allocated in this NAT pool.

Monitoring DHCP

A Services Router can operate as a DHCP server. To view information about dynamic and static DHCP leases, conflicts, pools, and statistics, select **Monitor > DHCP** in the J-Web interface or enter the following CLI commands:

- show system services dhcp binding
- show system services dhcp conflict
- show system services dhcp pool
- show system services dhcp statistics

In addition, you can display the globally configured DHCP settings by using the `show system services global` command from the CLI.

Table 65 summarizes the output fields in DHCP displays.

Table 65: Summary of DHCP Output Fields

Field	Values	Additional Information
DHCP Leases		
Allocated Address	List of IP addresses the DHCP server has assigned to clients.	
MAC Address	Corresponding media access control (MAC) address of the client.	
Binding Type	Type of binding assigned to the client: dynamic or static .	DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.
Lease Expires	Date and time the lease expires, or never for leases that do not expire.	
DHCP Conflicts		
Detection Time	Date and time the client detected the conflict.	
Detection Method	How the conflict was detected.	Only client-detected conflicts are displayed.
Address	IP address where the conflict occurs.	The addresses in the conflicts list remain excluded until you use the <code>clear system services dhcp conflict</code> command to manually clear the list.
DHCP Pools		
Pool Name	Subnet on which the IP address pool is defined.	
Low Address	Lowest address in the IP address pool.	
High Address	Highest address in the IP address pool.	
Excluded Addresses	Addresses excluded from the address pool.	
DHCP Statistics		
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.	
Packets dropped	Total number of packets dropped and the number of packets dropped due to a particular condition.	

Table 65: Summary of DHCP Output Fields (continued)

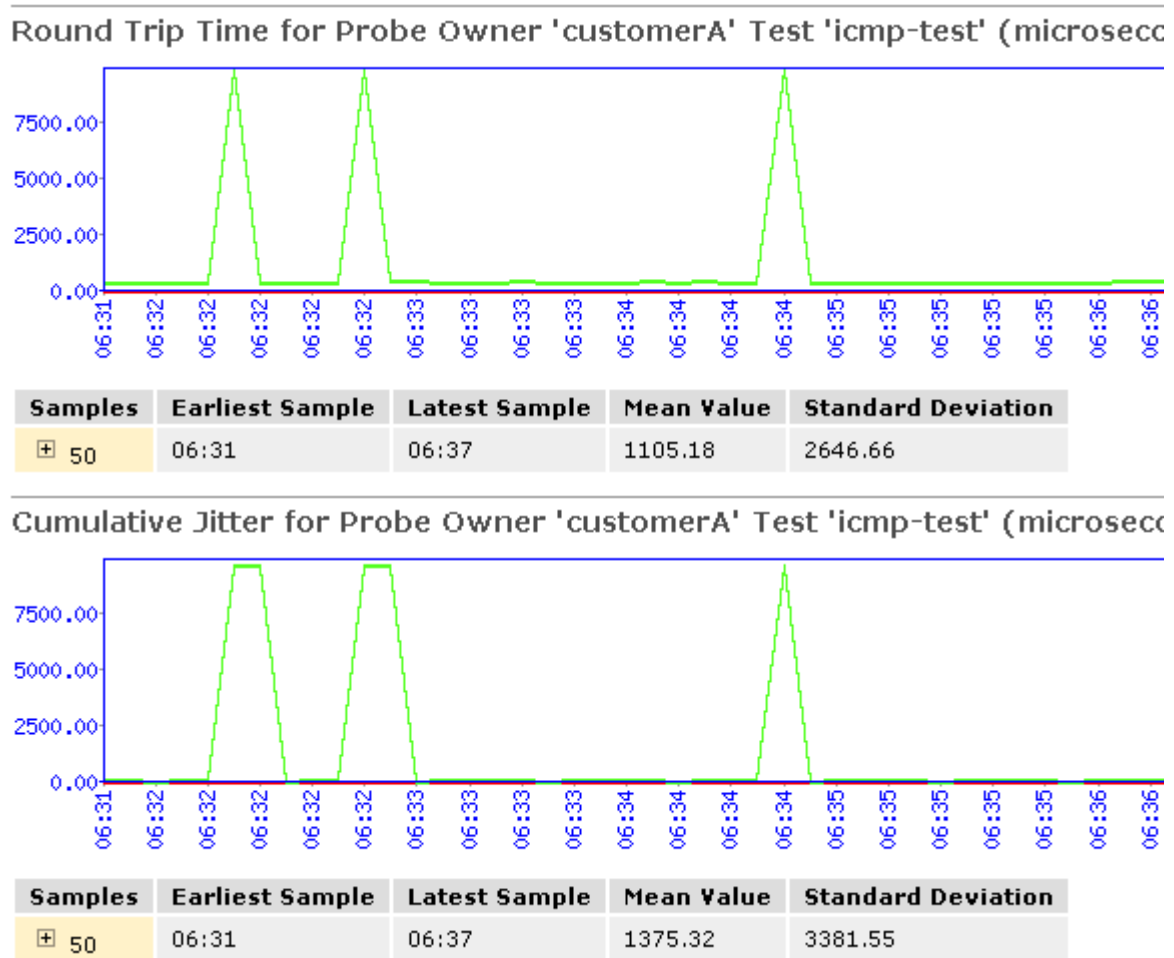
Field	Values	Additional Information
Messages received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.	
Messages sent	Number of BOOTREPLY, DHCPACK, DHCPOFFER, and DHCPNAK messages sent from the DHCP server to DHCP clients.	

Monitoring RPM Probes

The RPM information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the Services Router. To view these RPM properties, select **Monitor > 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 9 shows sample graphs for an RPM test.

Figure 9: Sample RPM Graphs

In Figure 9, 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 66 summarizes key output fields in RPM displays.

Table 66: 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.	

Table 66: Summary of Key RPM Output Fields (continued)

Field	Values	Additional Information
Test Name	Configured name of the RPM test.	
Probe Type	Type of RPM probe configured for the specified test. 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 Services Router to the remote server, as measured over the course of the test.	
Maximum RTT	Longest round-trip time from the Services Router to the remote server, as measured over the course of the test.	
Average RTT	Average round-trip time from the Services Router to the remote server, as measured over the course of the test.	
Standard Deviation RTT	Standard deviation of round-trip times from the Services Router 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 Services Router 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 round-trip time for the 50-probe sample.	

Table 66: Summary of Key RPM Output Fields (continued)

Field	Values	Additional Information
Standard Deviation	Standard deviation of the round-trip times for the 50-probe sample.	
Lowest Value	Shortest round-trip time from the Services Router 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 Services Router 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 Services Router 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.	

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 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 Services Router, and the PPPoE version configured on the Services Router, select **Monitor > PPPoE** in the J-Web interface.

To view interface-specific properties in the J-Web interface, select the interface name on the PPPoE page.

Alternatively, enter the following CLI commands:

- `show pppoe interfaces`
- `show pppoe statistics`
- `show pppoe version`

Table 67 summarizes key output fields in PPPoE displays.

You can also view status information about the PPPoE interface by selecting **Monitor > Interfaces > pp0**. Alternatively, enter the `show interfaces pp0` command. For more information about key output fields, see “Monitoring the Interfaces” on page 89.

Table 67: Summary of Key PPPoE Output Fields

Field	Values	Additional Information
PPPoE Interfaces		
Interface	Name of the PPPoE interface.	Click the interface name to display PPPoE information for the interface.

Table 67: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
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 Services Router 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 refereed 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, fe-0/0/0.1.	
PPPoE Statistics		
Active PPPoE Sessions	Total number of active PPPoE sessions.	

Table 67: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
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.	

Table 67: Summary of Key PPPoE Output Fields (continued)

Field	Values	Additional Information
PPPoE Version		
Maximum Sessions	Maximum number of active PPPoE sessions the Services Router can support. The default is 256 sessions.	
PADI Resend Timeout	Initial time, (in seconds) the Services Router 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 Services Router 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 Services Router 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 Services Router 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.	

Chapter 6

Monitoring Events and Managing System Log Files

J-series Services Routers support 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.

This chapter contains the following topics. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

- System Log Message Terms on page 129
- System Log Messages Overview on page 130
- Before You Begin on page 134
- Configuring System Log Messages with a Configuration Editor on page 134
- Monitoring System Log Messages with the J-Web Event Viewer on page 137

System Log Message Terms

Before configuring and monitoring system log messages on Services Routers, become familiar with the terms defined in Table 68.

Table 68: System Log Message Terms

Term	Definition
event	Condition that occurs on a Services Router 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 69.

Table 68: 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 the 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 router functionality. The following are some key JUNOS processes:</p> <ul style="list-style-type: none"> ■ Routing protocol process—Controls the routing protocols that run on a Services Router. It starts the configured routing protocols, handles all routing messages, maintains routing tables and implements the routing policy. ■ Interface process—Allows you to configure and control the physical and logical interfaces present in a Services Router. It also enables the JUNOS software to track the status and condition of the router's interfaces. ■ Chassis process—Allows you to configure and control the physical properties of a Services Router, including conditions that trigger alarms. ■ SNMP—Simple Network Management Protocol, which helps administrators monitor the state of a router. ■ Management process—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 the JUNOS software. It also starts all the software processes and the CLI when the router starts up. If a software process terminates, the management process attempts to restart it. <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.
regular expressions	Set of key combinations that allow you to have control over what you are searching. You can use regular expressions to filter system log messages by specifying a text string that must (or must not) appear in a message for the message to be logged. For more information, see "Regular Expressions" on page 132.
severity level	Measure of how seriously a triggering event affects Services Router functions. For a list of severity levels that you can specify, see Table 70.

System Log Messages Overview

The JUNOS software generates system log messages to record events that occur on the Services Router, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database

- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as router 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 134.
- To direct messages to the terminal session of one or more specific users (or all users) when they are logged into the router, see “Sending System Log Messages to a User Terminal” on page 135.
- To direct messages to the router 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*.

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 69 lists the system logging facilities, and Table 70 lists the system logging severity levels. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Table 69: 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 70: 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.
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.

Regular Expressions

On the J-Web View Events page, you can use regular expressions to filter and display a set of messages for viewing. JUNOS supports POSIX Standard 1003.2 for extended (modern) UNIX regular expressions.

Table 71 specifies some of the commonly used regular expression operators and the terms matched by them. A term can match either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces. For information about how to use regular expression to filter system log messages, see “Filtering System Log Messages” on page 138.



NOTE: On the J-Web View Events page, the regular expression matching is case-sensitive.

Table 71: Common Regular Expression Operators and the Terms They Match

Regular Expression Operator	Matching Terms
.	One instance of any character except the space. For example, <code>.in</code> matches messages with <i>win</i> or <i>windows</i> .
*	Zero or more instances of the immediately preceding term. For example, <code>tre*</code> matches messages with <i>tree</i> , <i>tread</i> or <i>trough</i> .
+	One or more instances of the immediately preceding term. For example, <code>tre+</code> matches messages with <i>tree</i> or <i>tread</i> but not <i>trough</i> .
?	Zero or one instance of the immediately preceding term. For example, <code>colou?r</code> matches messages with or <i>color</i> or <i>colour</i> .
	One of the terms that appear on either side of the pipe operator. For example, <code>gre ay</code> matches messages with either <i>grey</i> or <i>gray</i> .
!	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is specific to JUNOS.
^	The start of a line, when the caret appears outside square brackets. For example, <code>^T</code> matches messages with <i>This line</i> and not with <i>On this line</i> .
\$	Strings at the end of a line. For example, <code>:\$</code> matches messages with <i>the following:</i> and not with <i>2:00</i> .
[]	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, <code>[0-9]</code> matches messages with any number.
()	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression. For example, <code>dev(/ ice)</code> matches messages with <i>dev/</i> or <i>device</i> .

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 router.
- Configure network interfaces. See the *J-series Services Router Basic LAN and WAN Access 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 134
- Sending System Log Messages to a User Terminal on page 135
- Archiving System Logs on page 136
- Disabling System Logs on page 136

Sending System Log Messages to a File

You can direct system log messages to a file on the compact flash drive. The default directory for log files is `/var/log`. To specify a different directory on the compact flash drive, include the complete pathname. For the list of logging facilities and severity levels, see Table 69 and Table 70.

For information about archiving log files, see “Archiving System Logs” on page 136.

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 72.
3. If you are finished configuring the network, commit the configuration.

Table 72: 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Configure or Edit. 3. Next to Syslog, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system syslog
Create a file named security , and send log messages of the authorization class at the severity level info to the file.	<ol style="list-style-type: none"> 1. Next to File, click Add new entry. 2. In the File name box, type security. 3. Next to Contents, click Add new entry. 4. In the Facility list, select authorization. 5. In the Level list, select info. 	Set the filename and the facility and severity level: set file security authorization info

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 69 and Table 70.

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 73.
3. If you are finished configuring the network, commit the configuration.

Table 73: 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 Configuration > View and Edit > Edit Configuration. 2. Next to System, click Configure or Edit. 3. Next to Syslog, click Configure or Edit. 	From the [edit] hierarchy level, enter edit system syslog
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. 	Set the filename and the facility and severity level: set user frank any critical

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

You can use the J-Web interface to filter and view system log messages on a Services Router. To view system log messages, click **Events** in the J-Web task bar. (To view system log messages with the CLI, use the `show log` command.)

Figure 10 shows the Filter and Event Summary sections in the View Events page.

To monitor system log messages with an Event Viewer, perform the following tasks:

- Filtering System Log Messages on page 138
- Viewing System Log Messages on page 140

Figure 10: View Events Page

View Events

Filters

System Log File: ?

Event ID: ?

Text in Event Description: ?

Process: ?

Start Time: ?

End Time: ?

Number of Events to Display:

Event Summary

Showing events 1 to 25 of 55

[Next >](#) [Last >>](#)

Time	Process	Event ID	Event Description
2006-03-27 23:10:50 PST	mgd[4231]	UI_CHILD_EXITED ?	Child exited: PID 4244, status 4, command '/sbin/disklabel'
2006-03-27 23:10:50 PST	mgd[4231]	UI_CHILD_EXITED ?	Child exited: PID 4243, status 4, command '/sbin/disklabel'
2006-03-27 23:10:49 PST	checklogin[4229]	WEB_AUTH_SUCCESS	Authenticated httpd client (username regress)
2006-03-27 23:10:10 PST	inetd[2963]		/usr/libexec/telnetd[4198]: exited, status 1
2006-03-27 23:10:08 PST	su		regress to root on /dev/tty0
2006-03-27 23:10:04 PST	login	LOGIN_INFORMATION	User regress logged in from host 192.168.5.86 on device tty0
2006-03-27 23:08:23 PST	mgd[4135]	UI_CHILD_EXITED ?	Child exited: PID 4148, status 4, command '/sbin/disklabel'
2006-03-27 23:08:23 PST	mgd[4135]	UI_CHILD_EXITED ?	Child exited: PID 4147, status 4, command '/sbin/disklabel'
2006-03-27 23:08:22 PST	checklogin[4133]	WEB_AUTH_SUCCESS	Authenticated httpd client (username regress)
2006-03-27 23:07:29 PST	mib2d[2974]	SNMP_TRAP_LINK_DOWN ?	ifIndex 30, ifAdminStatus up(1), ifOperStatus down(2), ifName fe-0/0/
2006-03-27 23:03:46 PST	inetd[2963]		/usr/libexec/telnetd[4069]: exited, status 1
2006-03-27 23:03:44 PST	su		regress to root on /dev/tty0

Filtering System Log Messages

You can use filters to display relevant events. Table 74 describes the different filters, their functions, and the associated actions. You can apply any or a combination of the described filters to view the messages that you want to view.

Table 74: Filtering System Log Messages

Field	Function	Your Action
System Log File	<p>Specifies the name of a system log file for which you want to display the recorded events.</p> <p>Lists the names of all the system log files that you configure.</p> <p>By default, a log file, messages, is included in the /var/log/ directory.</p> <p>For information about how to configure system log files, see “Sending System Log Messages to a File” on page 134.</p>	To specify events recorded in a particular file, select the system log filename from the list—for example, messages .
Event ID	<p>Specifies the Event ID for which you want to display the messages.</p> <p>Allows you to type part of the ID and completes the remaining automatically.</p> <p>An event ID, also known as system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.</p>	To specify events with a specific ID, type its partial or complete ID—for example, TFTPD_AF_ERR .
Text in Event Description	<p>Specifies text from the description of events that you want to display.</p> <p>Allows you to use regular expression to match text from the event description.</p> <p>NOTE: The regular expression matching is case sensitive.</p> <p>For more information about using regular expressions, see “Regular Expressions” on page 132.</p>	<p>To specify events with a specific description, type a text string from the description with regular expression.</p> <p>For example, type ^Initial* to display all messages with lines beginning with the term <i>Initial</i>.</p>
Process	<p>Specifies the name of the process generating the events you want to display.</p> <p>To view all the processes running on your system, enter the CLI command—show system processes.</p> <p>For more information about processes, see the <i>JUNOS Software Installation and Upgrade Guide</i>.</p>	<p>To specify events generated by a process, type the name of the process.</p> <p>For example, type mgd to list all messages generated by the management process.</p>

Table 74: Filtering System Log Messages (continued)

Field	Function	Your Action
Start Time	Specifies the time period in which the events you want displayed are generated.	To specify the time period:
End Time	Displays a calendar that allows you to select the year, month, day, and time. It also allows you to select the local time. By default, the messages generated in the last one hour are displayed—End Time shows the current time and Start Time shows the time one hour before end time.	<ul style="list-style-type: none"> Click the box next to Start Time and select the year, month, date, and time—for example, 02/10/2006 11:32. Click the box next to End Time and select the year, month, date, and time—for example, 02/10/2006 3:32. <p>To select the current time as the start time, select local time.</p>
Number of Events to Display	Specifies the number of events to be displayed on the View Events page. By default, the View Events page displays 25 events.	To view a specified number of events, select the number from the list—for example, 50 .
OK	Applies the specified filter and displays the matching messages.	To apply the filter, click OK .

Viewing System Log Messages

By default, the View Events page displays the most recent 25 events, with severity levels highlighted in different colors. After you specify the filters, Event Summary displays the events matching the specified filters. Click **First**, **Next**, **Prev**, and **Last** links to navigate through messages. Table 75 describes the Event Summary fields.

Table 75: Viewing System Log Messages

Field	Function	Additional Information
Time	Displays the time at which the message was logged.	
Process	Displays the name and ID of the process that generated the system log message.	

Table 75: Viewing System Log Messages (continued)

Field	Function	Additional Information
Event ID	<p>Displays a code that uniquely identifies the message.</p> <p>The prefix on each code identifies the message source, and the rest of the code indicates the specific event or error.</p> <p>Displays context-sensitive help that provides more information about the event:</p> <ul style="list-style-type: none"> ■ Help—Short description of the message. ■ Description—More detailed explanation of the message. ■ Type—Category to which the message belongs. ■ Severity—Level of severity. 	<p>The event ID begins with a prefix that indicates the generating software process.</p> <p>Some processes on a Services Router do not use codes. This field might be blank in a message generated from such a process.</p> <p>An Event can belong to one of the following Type categories:</p> <ul style="list-style-type: none"> ■ Error—Indicates an error or failure condition that might require corrective action. ■ Event—Indicates a condition or occurrence that does not generally require corrective action.

Table 75: Viewing System Log Messages (continued)

Field	Function	Additional Information
Event Description	Displays a more detailed explanation of the message.	
Severity	<p>Severity level of a message is indicated by different colors.</p> <ul style="list-style-type: none"> ■ Unknown—Gray—Indicates no severity level is specified. ■ 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. 	<p>A severity level indicates how seriously the triggering event affects routing platform functions. When you configure a location for logging a facility, you also specify a severity level for the facility. Only messages from the facility that are rated at that level or higher are logged to the specified file.</p>

Chapter 7

Configuring and Monitoring Alarms

Alarms on a J-series Services Router alert you to conditions on a network interface, on the router chassis, or in the system software that might prevent the router 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 router. You can monitor active alarms from the J-Web interface or the CLI.

This chapter contains the following topics. For more information about alarms, see the *JUNOS System Basics Configuration Guide*.

- Alarm Terms on page 143
- Alarm Overview on page 144
- Before You Begin on page 150
- Configuring Alarms with a Configuration Editor on page 150
- Checking Active Alarms on page 152
- Verifying the Alarms Configuration on page 154

Alarm Terms

Before configuring and monitoring alarms on Services Routers, become familiar with the terms defined in Table 76.

Table 76: Alarm Terms

Term	Definition
alarm	Signal alerting you to conditions that might prevent normal operation. On a Services Router, 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).
chassis alarm	Predefined alarm triggered by a physical condition on the router such as a power supply failure, excessive component temperature, or media failure.

Table 76: Alarm Terms (continued)

Term	Definition
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 service (IDS), 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

Services Router alarms warn you about conditions that can prevent the router from operating normally.

When an alarm condition triggers an alarm, the Services Router lights the yellow (amber) ALARM LED on the front panel. When the condition is corrected, the light turns off.



NOTE: The ALARM LED on the Services Router lights yellow whether the alarm condition is major (red) or minor (yellow).

This section contains the following topics:

- Alarm Types on page 144
- Alarm Severity on page 145
- Alarm Conditions on page 145

Alarm Types

The Services Router 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 router or one of its component. 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 on a Services Router have two severity levels:

- Major (red)—Indicates a critical situation on the router 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 router 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 Services Router 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.

This section contains the following topics:

- Interface Alarm Conditions on page 145
- Chassis Alarm Conditions and Corrective Actions on page 148
- System Alarm Conditions and Corrective Actions on page 149

Interface Alarm Conditions

Table 77 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, IDS, and IPSec, which operate on an internal adaptive services module within a Services Router, you can configure alarm conditions on the integrated services and services interfaces.

Table 77: Interface Alarm Conditions

Interface	Alarm Condition	Description	Configuration Option
DS1 (T1)	Alarm indication signal	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 red alarm failure. This condition is also known as a far end alarm failure.	ylw
Ethernet (Fast 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 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 signal absent	The remote endpoint of the serial link is not transmitting a DCD signal. Because the DCD signal transmits the state of the router, no signal probably indicates that the remote endpoint of the serial link is unavailable.	dcd-absent
	Data Set Ready 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 77: Interface Alarm Conditions (continued)

Interface	Alarm Condition	Description	Configuration Option
Services	Services module hardware down	A hardware problem has occurred on the Services Router'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 Services Router and its services module is unavailable.	linkdown
	Services module held in reset	The Services Router'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 Services Router'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 Services Router's services module.	sw-down
E3	Alarm indication signal	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	No remote E3 signal is being received at the E3 interface.	los
	Out of frame	An out-of-frame (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 77: 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	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 out-of-frame (OOF) or loss-of-signal (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	An out-of-frame (OOF) or loss-of-signal (LOS) condition has existed for 10 seconds. The loss-of-frame (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 red alarm failure. This condition is also known as a far end alarm failure.	ylw

Chassis Alarm Conditions and Corrective Actions

Table 78 lists chassis components with preset alarms, the conditions that can trigger an alarm, the alarm severity, and the action you take to correct the condition.

Table 78: Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Corrective Action	Alarm Severity
Alternative boot media	The Services Router boots from an alternative boot device—the removable compact flash disk or the USB storage device.	Typically, the router boots from the primary compact flash disk. If you configured your router to boot from an alternative boot device, ignore this alarm condition. If you did not configure the router to boot from an alternative boot device, contact JTAC. (See “Requesting Support” on page xx.)	Yellow (minor)
PIM	A PIM has failed. When a PIM fails, it attempts to reboot. If the Routing Engine detects that a PIM is rebooting too often, it shuts down the PIM.	Replace the failed PIM. (See the Getting Started Guide for your router.)	Red (major)
Routing Engine	An error occurred during the process of reading or writing compact flash.	Reformat the compact flash and install a bootable image. (See “Performing Software Upgrades and Reboots” on page 159.) If this remedy fails, you must replace the failed Routing Engine. To contact JTAC, see “Requesting Support” on page xx.	Yellow (minor)
	Routing Engine temperature is too warm.	■ Check the room temperature. (See the Getting Started Guide for your router.)	Yellow (minor)
	Routing Engine temperature is too hot.	■ Check the air flow. (See the Getting Started Guide for your router.) ■ Check the fans. (See the Getting Started Guide for your router .) If you must replace a fan or the Routing Engine, contact JTAC. (See “Requesting Support” on page xx.)	Red (major)
	Routing Engine fan has failed.	Replace the failed fan. To contact JTAC, see “Requesting Support” on page xx.	Red (major)

System Alarm Conditions and Corrective Actions

Table 79 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 79: 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>J-series Services Router Basic LAN and WAN Access Configuration Guide</i> .
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 Getting Started Guide for your router.

Before You Begin

Before you begin configuring and monitoring alarms, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your router.
- Configure network interfaces. See the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Configuring Alarms with a Configuration Editor

To configure interface alarms on a Services Router, you must select the network interface on which to apply an alarm and the condition you to trigger the alarm. For a list of conditions, see “Interface Alarm Conditions” on page 145.

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 80.
3. If you are finished configuring the network, commit the configuration.
4. To verify the alarms configuration, see “Displaying Alarm Configurations” on page 154.
5. To check the status of active alarms, see “Checking Active Alarms” on page 152.

Table 80: 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 Configuration > View and Edit > Edit Configuration. 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
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 the Ylw list, select red. 3. Click OK. 	Enter set ds1 ylw red
Configure the system to generate a red interface alarm when a link down failure is detected on a Fast 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. 	Enter set ethernet link-down red
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

Table 80: Configuring Interface Alarms (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the system to generate the following interface alarms on a T3 link:	1. In the T3 field, click Configure .	1. Enter
■ Red alarm when the remote endpoint is experiencing a Red failure	2. From the Ylw list, select red .	set t3 ylw red
■ Yellow alarm when the upstream bit stream has more consecutive zeros than are permitted	3. From the Exz list, select yellow .	2. Enter
	4. From the Los list, select red .	set t3 exz yellow
■ Red alarm when there is a loss of signal on the interface	5. Click OK .	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 router.	1. On the main Configuration page next to System, click Configure or Edit .	1. Enter
To define login classes, see the <i>JUNOS System Basics Configuration Guide</i> .	2. Next to Login, click Configure or Edit .	edit system login
	3. In the Class field, click Add new entry .	2. Enter
	4. In the Class name field, type admin .	set class admin login-alarms
	5. Select the Login alarms check box.	
	6. Click OK .	

Checking Active Alarms

The alarm information includes alarm type, alarm severity, and a brief description for each active alarm on the Services Router. To view the active alarms, select **Alarms** in the J-Web interface, or enter the following CLI show commands:

- show chassis alarms
- show system alarms



NOTE: If a Services Router has active alarms and you have not displayed the View Alarms page, *Alarms* in the task bar appears in red. After you view the alarms, *Alarms* returns to grey. If new alarms become active, *Alarms* is red until you again display the View Alarms page.

Figure 11 shows the View Alarms summary page. Click an alarm in the list of active alarms to display a detailed alarm message.

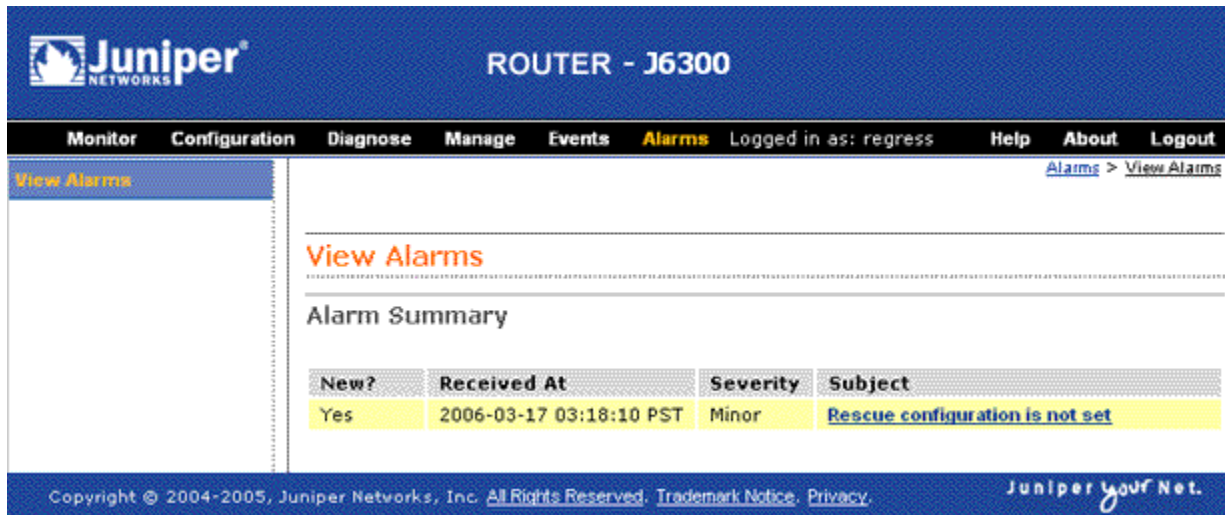
Figure 11: J-Web View Alarms Summary Page

Table 81 summarizes the output fields on the alarms page.

Table 81: Summary of Key Alarm Output Fields

Field	Values	Additional Information
Alarm Summary		
New?	Viewed status of the alarm—either Yes (a new alarm) or No (a previously viewed alarm).	After you have once displayed the View Alarms page, any new alarms that appear on the page during the same J-Web session are identified as previously viewed.
Received at	Date and time when the alarm condition was detected.	
Severity	Alarm severity—either major (red) or minor (yellow).	A major (red) alarm condition requires immediate action. A minor (yellow) condition requires monitoring or maintenance.
Subject	Brief synopsis of the alarm.	Clicking the alarm subject displays a detailed alarm message.
Detailed Alarm Message		
Received at	Date and time when the failure was detected.	

Table 81: Summary of Key Alarm Output Fields (continued)

Field	Values	Additional Information
Severity	Alarm severity—either major (red) or minor (yellow).	A major (red) alarm condition requires immediate action. A minor (yellow) condition requires monitoring or maintenance.
Alarm Type	Category of the alarm: <ul style="list-style-type: none"> ■ Chassis—Indicates an alarm condition on the chassis (typically an environmental alarm such as temperature) ■ Configuration—Indicates that no rescue configuration is set ■ ETHER—Indicates an alarm condition on a Fast Ethernet interface ■ DS3—Indicates an alarm condition on a DS3 interface ■ License—Indicates a software license infringement ■ Serial—Indicates an alarm condition on a serial interface ■ Services—Indicates an alarm condition on the services module 	

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 Configuration > View and Edit > View Configuration Text . Alternatively, from configuration mode in the CLI, enter the <code>show chassis alarms</code> command.
Sample Output	<pre>[edit] user@host# show chassis alarms t3 { exz yellow; los red; ylw red; } ds1 { ylw red;</pre>

```
}  
ethernet {  
    link-down red;  
}  
serial {  
    loss-of-rx-clock red;  
    loss-of-tx-clock red;  
    dcd-absent yellow;  
    cts-absent yellow;  
}
```

What It Means 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
- Fast Ethernet alarms
- Serial alarms

For more information about the format of a configuration file, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Part 3

Managing Services Router Software

- Performing Software Upgrades and Reboots on page 159
- Managing Files on page 183

Chapter 8

Performing Software Upgrades and Reboots

A J-series Services Router is delivered with the JUNOS Internet software preinstalled. When you power on the router, it starts (boots) up using its primary boot device. All Services Routers 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 in case it becomes corrupted or fails during the upgrade.

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

If the router has no secondary boot device configured and the primary boot device becomes corrupted, you can reload the JUNOS recovery software package onto the corrupted compact flash disk with either a UNIX or Microsoft Windows computer.

Use either the J-Web interface or the CLI to schedule a reboot or system halt on the router, or to perform one immediately.

This chapter contains the following topics. For more information about installing and upgrading JUNOS software, see the *JUNOS Software Installation and Upgrade Guide*.

- Upgrade and Downgrade Overview on page 160
- Before You Begin on page 161
- Downloading Software Upgrades from Juniper Networks on page 162
- Installing Software Upgrades on page 162
- Downgrading the Software on page 166
- Configuring Boot Devices on page 167
- Recovering Primary Boot Devices on page 173

- Rebooting or Halting a Services Router on page 177

Upgrade and Downgrade Overview

Typically, you upgrade the JUNOS Internet software on a Services Router by downloading a set of images onto your router or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the J-Web interface or the CLI. Finally, you boot your system with this upgraded device.

A JUNOS software package is a collection of files that make up a software component. You can download software packages either for upgrading JUNOS software or for recovering a primary compact flash.

All JUNOS software is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1) checksums, and Message Digest 5 (MD5) checksums. For more information about JUNOS software packages, see the *JUNOS Installation and Upgrade Guide*.

Upgrade Software Packages

Download an upgrade software package, also known as an install package, to install new features and software fixes as they become available.

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-jseries*.
- *m.n* is the software release, with *m* representing the major release number—for example, 7.5.
- *Z* indicates the type of software release. For example, *R* indicates released software, and *B* indicates beta-level software.
- *x* represents the version of the major software release—for example, 2.
- *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-jseries-7.5R2-domestic.tgz*.

Recovery Software Packages

Download a recovery software package, also known as an install media package, to recover a primary compact flash device.

A recovery software package name is in the following format:

package-name-m.nZx-export-cf nnn .gz.

- *package-name* is the name of the package—for example, *junos-jseries*.
- *m.n* is the software release, with *m* representing the major release number—for example, 7.5.
- *Z* indicates the type of software release. For example, *R* indicates released software, and *B* indicates beta-level software.
- *x* represents the version of the major software release—for example, 2.
- *export* indicates that the recovery software package is the exported worldwide software package version.
- *cf nnn* indicates the size of the target compact flash device in megabytes—for example, *cf256*.

A sample J-series recovery software package name is *junos-jseries-7.5R2-export-cf256.gz*.

Before You Begin

To download software upgrades, you must have a Web account with Juniper Networks. To obtain an account, complete the registration form at the Juniper Networks Web site: <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 router is 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 rebuilds the file system but retains configuration files, log files, and similar information from the previous version.



NOTE: For media redundancy, we recommend that you keep a secondary storage medium attached and updated at all times. For instructions, see “Configuring Boot Devices” on page 167.

Use either the J-Web interface or the CLI to back up the primary boot device on one of the secondary storage devices listed in Table 82.

Table 82: Secondary Storage Devices for Backup

Storage Device	Available on Routers	Minimum Storage Required
Removable compact flash disk	J4300 and J6300	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 168. For instructions about how to backup your system using the CLI, see “Configuring a Boot Device for Backup with the CLI” on page 171.

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 Web page. 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 authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using either the J-Web interface or the CLI, select the appropriate junos-j-series software package for your application. For information about JUNOS software packages, see “Upgrade and Downgrade Overview” on page 160.
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 install JUNOS software upgrades. This section contains the following topics:

- Installing Software Upgrades with the J-Web Interface on page 163
- Installing Software Upgrades with the CLI on page 166

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 by uploading the file to the router. This section contains the following topics:

- Installing Software Upgrades from a Remote Server on page 163
- Installing Software Upgrades by Uploading Files on page 164

Installing Software Upgrades from a Remote Server

You can use the J-Web interface to install software packages on the Services Router that are retrieved with FTP or HTTP from the location specified.

Figure 12 shows the Install Remote page for the router.

Figure 12: Install Remote Page

The screenshot displays the Juniper J-Web interface for a J4300 router. The top navigation bar includes links for Monitor, Configuration, Diagnose, Manage (highlighted), Events, Logged in as: regress, Help, About, and Logout. The left sidebar contains links for Files, Software (highlighted), Licenses, Reboot, and Snapshot. The main content area is titled 'Software' and 'Install Package'. It contains the following fields and controls:

- Package Location:** A text input field with a help icon.
- User:** A text input field with a help icon.
- Password:** A text input field with a help icon.
- Reboot If Required:** A checkbox with a help icon.
- Buttons:** 'Fetch and Install Package' and 'Cancel'.

The footer of the page includes copyright information: Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. and the Juniper logo with the tagline 'Juniper your Net.'.

To install software upgrades from a remote server:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 162.
2. In the J-Web interface, select **Manage > Software > Install Package**.
3. On the Install Remote page, enter information into the fields described in Table 83.
4. Click **Fetch and Install Package**. The software is activated after the router has rebooted.

Table 83: Install Remote Summary

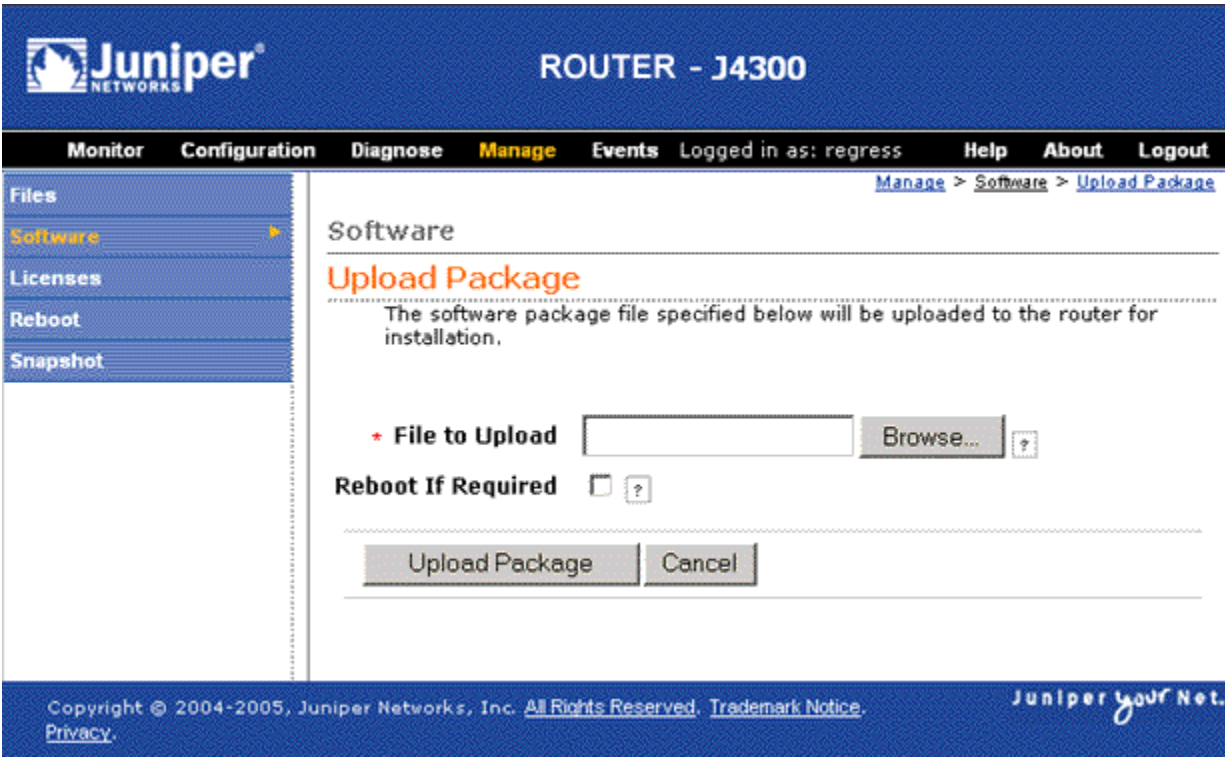
Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name.	Type the full address of the software package location on the FTP or HTTP server—one of the following: <code>ftp:// hostname / pathname / package-name</code> <code>http:// hostname / 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 router is automatically rebooted when the upgrade is complete.	Check the box if you want the router 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 to the Services Router.

Figure 13 shows the Upload Package page for the router.

Figure 13: Upload Package Page



To install software upgrades by uploading files:

- 1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 162.
- 2. In the J-Web interface, select **Manage > Software > Upload Package**.
- 3. On the Upload Package page, enter information into the fields described in Table 84.
- 4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 84: Upload Package Summary

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

Installing Software Upgrades with the CLI

To install software upgrades on a router with the CLI:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 162.
2. Copy the software package to the router. We recommend that you copy it to the `/var/tmp` directory.
3. Install the new package on the Services Router:

```
user@host> request system software add validate unlink reboot source
```

Replace `source` with one of the following paths:

- For a software package that is installed from a local directory on the router—`/pathname/package-name`
- For software packages that are downloaded and installed from a remote location:
 - `ftp://hostname/pathname/package-name`
 - `http://hostname/pathname/package-name`

The `validate` option validates the software package against the current configuration as a prerequisite to adding the software package, to ensure that the router reboots successfully. This is the default behavior when you are adding a software package for a different release.

The `unlink` option removes the package at the earliest opportunity so that the router has enough room to complete the installation.

Adding the `reboot` command reboots the router after the upgrade is validated and installed. Rebooting takes place only if the upgrade is successful.

When the reboot is complete, the router displays the login prompt.

Downgrading the Software

Downgrade the JUNOS software on the Services Router with either the J-Web interface or the CLI. This section contains the following topics:

- Downgrading the Software with the J-Web Interface on page 167
- Downgrading the Software with the CLI on page 167

Downgrading the Software with the J-Web Interface

You can downgrade the software from the J-Web interface. When you downgrade the software to a previous version, the software version that is saved in `junos.old` is the version of JUNOS that your router is downgraded to. For your changes to take effect, you must reboot the router.

To downgrade software:

1. Go to **Manage > Software > Downgrade**. The previous version (if any) is displayed on this page. For example, you can downgrade to the previously installed version of the router software, `/cf/packages/junos-7.0120040930_1745-domestic`.



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 **Manage > Reboot** to reboot the router at your convenience.

Downgrading the Software with the CLI

You can revert to the previous set of software using the `request system software rollback` command in the CLI. Rollback fails if the `junos-jseries` software bundle cannot be found in `/var/sw/pkg`.

You can roll back only to the software release that was installed on the Services Router before the current release. After you issue the `request system software rollback` command, the old release is loaded and you cannot reload it again. Issuing the `request system software rollback` command again results in an error.

To downgrade to an earlier version of software, follow the procedure for upgrading, using the `junos-jseries` software bundle labeled for the appropriate release.

Configuring Boot Devices

You can configure a boot device to replace the primary boot device on your Services Router, 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 router, 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 Services Router and updated at all times.

If the primary storage medium becomes corrupted and no backup medium is in place, you can recover the primary compact flash from a special JUNOS 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 Getting Started Guide for your router.

This section contains the following topics:

- Configuring a Boot Device for Backup with the J-Web Interface on page 168
- Configuring a Boot Device for Backup with the CLI on page 171
- Configuring a Boot Device to Receive Software Failure Memory Snapshots on page 173

Configuring a Boot Device for Backup with the J-Web Interface

You can use the J-Web interface to create a boot device for the Services Router on an alternate medium, to replace the primary boot device or serve as a backup.

Figure 14 shows the Snapshot page.

Figure 14: Snapshot Page

Juniper
NETWORKS

ROUTER - J4300

Monitor Configuration Diagnose **Manage** Events Logged in as: regress Help About Logout

Files
Software
Licenses
Reboot
Snapshot

[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 ?

Factory ☐ ?

Partition ☐ ?

☒ **Advanced options**

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) Juniper your Net.

To create a boot device:

1. In the J-Web interface, select **Manage > Snapshot**.
2. On the Snapshot page, enter information into the fields described in Table 85.
3. Click **Snapshot**.
4. Click **OK**.

Table 85: 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 primary compact flash drive. ■ removable-compact-flash—Copies software to the removable compact flash drive. This option is available on J4300 and J6300 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 primary compact flash drive 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 a primary compact flash drive 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 a removable 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 primary compact flash drive or to replicate it for use in another Services Router. This process also partitions the boot medium.</p> <p>NOTE: After the boot device is created as a primary compact flash drive, it can operate only in a primary compact flash drive slot.</p>	<p>To create a boot medium to use in the primary compact flash drive only, select the check box.</p>
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 router, and can be used for extra storage.</p> <p>This selection also partitions the boot medium.</p>	<p>Type a numeric value, in kilobytes. The default value is 0 KB.</p>

Table 85: Snapshot Summary (continued)

Field	Function	Your Action
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 173.</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 for the Services Router 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 86 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 86: CLI request system snapshot Command Options

Option	Description
as-primary	<p>On a removable compact flash 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 primary compact flash drive or to replicate it for use in another Services Router. This process also partitions the boot medium.</p> <p>NOTE: After the boot device is created as a primary compact flash drive, it can operate only in a primary compact flash drive slot.</p>
config-size <i>size</i>	<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 <i>size</i>	<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 router, 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 primary compact flash drive 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 primary compact flash drive slot.</p>
media <i>type</i>	<p>Specifies the boot device the software snapshot is copied to:</p> <ul style="list-style-type: none"> ■ compact-flash—Copies software to the primary compact flash drive. ■ removable-compact-flash—Copies software to the removable compact flash drive. This option is available on J4300 and J6300 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 <i>size</i>	<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>
swap-size <i>size</i>	<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 173.</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 Services Router 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 router 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 router (`/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 87 describes the `set system dump-device` command options.

Table 87: 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 primary compact flash as the system software failure memory snapshot device.
removable-compact-flash	Uses the compact flash device on the front of the router (J4300 and J6300 only) as the system software failure memory snapshot device.
usb	Uses the device attached to the USB port as the system software failure memory snapshot device.

Recovering Primary Boot Devices

All Services Routers use a compact flash disk, or card, to store the JUNOS Internet software, router configuration files, and log files. The primary compact flash drive is not hot-swappable and is accessible only after you remove the cover on the back panel of the router chassis. In addition to the primary compact flash disk, J4300 and J6300 Services Routers have a slot in the front of the chassis for removable flash media. All Services Routers also support externally pluggable USB storage devices. If the primary storage medium becomes corrupted and no secondary medium is in place, you can reload the JUNOS recovery software package onto the

corrupted compact flash card with a desktop or laptop computer running either a UNIX, Microsoft Windows 2000, or Windows XP operating system.

This section contains the following topics:

- Why Compact Flash Recovery Might Be Necessary on page 174
- Recommended Recovery Hardware and Software on page 174
- Configuring Primary Compact Flash Recovery on page 175

Why Compact Flash Recovery Might Be Necessary

For media redundancy, we recommend that you keep a secondary storage medium attached and updated at all times. Use the `request system snapshot` command to perform the update. (For instructions, see “Configuring Boot Devices” on page 167.)

If the primary compact flash disk fails at startup, the Services Router automatically boots itself from the removable compact flash or USB storage device. When a redundant storage medium is not available, the router is unable to boot and does not come back online. This situation can occur if the power fails during a JUNOS software upgrade and the physical or logical storage media on the router are corrupted.

If the primary storage medium becomes corrupted and no secondary medium is in place, you can reload the JUNOS software image onto the corrupted compact flash card with a desktop or laptop computer running either a UNIX, Microsoft Windows 2000, or Windows XP operating system.



CAUTION: This procedure does not recover any router configuration files. After you reinstall the JUNOS software, all the information on the original primary compact flash disk is lost.

Recommended Recovery Hardware and Software

Before configuring compact flash recovery, assemble the equipment and software listed in Table 88.

Table 88: Recommended Recovery Hardware and Software

Recommended Hardware and Software	Examples
Recovery Hardware	
Host system	Desktop or laptop PC equipped with a PCMCIA controller or USB port

Table 88: Recommended Recovery Hardware and Software (continued)

Recommended Hardware and Software	Examples
Adapter appropriate for your system	<ul style="list-style-type: none"> ■ For systems with PCMCIA controllers, a compact-flash-to-PCMCIA adapter—for example, a Macally PCM-CF compact flash PCMCIA adapter. ■ For systems with a USB port, a USB-to-compact-flash adapter. For example: <ul style="list-style-type: none"> ■ SIIG USB 2.0 Card Reader, model US2274, part number JU-CF0122 ■ MediaGear USB 2.0 Combo 9-in-4, model MGTR100 ■ AVP USB 8-in-1 Card Reader, model UC-28 ■ Inland Multi-Plus Card Reader, part number 08310 ■ HummingBird Multi Card Reader, HCR 81
Recovery Software	
Software appropriate for your system	<ul style="list-style-type: none"> ■ UNIX with PCMCIA drivers ■ Windows 2000, or Windows XP
Systems running Windows require additional software.	<ul style="list-style-type: none"> ■ WinZip, gzip, or a similar compression utility ■ A utility such as the following that allows you to write files to unformatted devices: <ul style="list-style-type: none"> ■ Norton Ghost ■ dd utility from the Cygwin package ■ physdiskwrite utility

Configuring Primary Compact Flash Recovery

To recover a primary compact flash disk with a corrupt or missing operating system, you must remove the corrupt primary compact disk from the J-series Services Router, plug it into a PC with a PCMCIA adapter or USB card reader, copy the JUNOS recovery software package onto it, and reinstall on the router. For instructions about how to remove and install primary compact flash disks, see the Getting Started Guide for your router.

Recovery software packages are available from the same location as J-series upgrade software packages. (See “Downloading Software Upgrades from Juniper Networks” on page 162.)

To recover a primary compact flash disk:

1. Plug the compact flash device into a PCMCIA adapter or USB card reader.
2. Plug the PCMCIA adapter or USB card reader into the host PC and verify that the compact flash is recognized by the operating system.
3. Select the appropriate recovery software package according to the size of your compact flash device. The uncompressed package must have the same size as the target compact flash capacity: 128 MB, 256 MB, 512 MB or 1024 MB.

The recovery software package name indicates the size of the package. For information about recovery software package names, see “Upgrade and Downgrade Overview” on page 160.

4. Copy the software package to a temporary directory on the host PC and uncompress it with a compression utility, such as WinZip.
5. Copy the uncompressed software package from the temporary directory to the compact flash device with one of the following commands:



CAUTION: You must use the correct target device name. Failure to do so might damage other storage devices connected to the host PC.

- On a UNIX PC, use the command `dd if=filename of=/dev/device_name`. Replace *filename* with the name of the uncompressed image, and *device_name* with the name of the unformatted PCMCIA card device. For example:

```
root# dd if=junos-jseries-7.0-20041028.0-export-cf128 of=/dev/hde
250368+0 records in 250368+0 records out
```

- On a Windows 2000 or Windows XP PC, use the Norton Ghost, dd, or physdiskwrite utility. The following example shows the use of physdiskwrite:

```
C:\> physdiskwrite -u junos-jseries-7.0-20041028.0-export-cf512

physdiskwrite v0.5 by Manuel Kasper
Searching for physical drives...
Information for \\.\PhysicalDrive0:
Windows: cyl: 2432
tpc: 255
spt: 63
C/H/S: 16383/16/63
Model: HITACHI_DK23DA-20
Serial number: 123ABC
Firmware rev.: 00J2A0G0
Information for \\.\PhysicalDrive1:
Windows: cyl: 125
tpc: 255
spt: 63
Which disk do you want to write? (0..1) 1
WARNING: that disk is larger than 800 MB! Make sure you're
not accidentally overwriting your primary hard disk!
Proceeding on your own risk...
About to overwrite the contents of disk 1 with new data.
Proceed? (y/n) y
511451136/511451136 bytes written in total
```



NOTE: The copy process can take several minutes.

After copying the software package to the compact flash device, you can use it as the primary compact flash disk in any J-series Services Router. For installation instructions, see the Getting Started Guide for your router.

Rebooting or Halting a Services Router

Reboot or halt a Services Router with either the J-Web interface or the CLI. This section contains the following topics:

- Rebooting or Halting a Services Router with the J-Web Interface on page 177
- Rebooting a Services Router with the CLI on page 180
- Halting a Services Router with the CLI on page 180

Rebooting or Halting a Services Router with the J-Web Interface

You can use the J-Web interface to schedule a reboot or halt the Services Router.

Figure 15 shows the Reboot page for the router.

Figure 15: Reboot Page

Juniper
NETWORKS

ROUTER - J4300

Monitor Configuration Diagnose **Manage** Events Logged in as: regress Help About Logout

[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 minutes
☐ Reboot when the system time is :
☐ Halt Immediately

Reboot From Media

Message

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) Juniper your Net.

To reboot or halt the router with the J-Web interface:

1. In the J-Web interface, select **Manage > Reboot**.
2. Select one of the following options:
 - **Reboot Immediately**—Reboots the router immediately.

- **Reboot in *number of minutes***—Reboots the router in the number of minutes from now that you specify.
 - **Reboot when the system time is *hour:minute***—Reboots the router 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 router software immediately. After the router software has stopped, you can access the router through the console port only.
3. Choose the boot device from the **Reboot from media** list:
 - **compact-flash**—Reboots from the primary compact flash drive. This selection is the default choice.
 - **removable-compact-flash**—Reboots from the optional removable compact flash drive. This selection is available on J4300 and J6300 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 router 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 router reboots. You cannot access the J-Web interface until the router has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
 - 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 router is halted, all software processes stop and you can access the router through the console port only. Reboot the router by pressing any key on the keyboard.



NOTE: If you cannot connect to the router through the console port, shut down the router by pressing and holding the power button on the front panel until the **POWER** LED turns off. After the router has shut down, you can power on the router by pressing the power button again. The **POWER** LED lights during startup and remains steadily green when the router is operating normally.

Rebooting a Services Router with the CLI

You can use the `request system reboot` CLI command to schedule a reboot of the Services Router:

```
user@host> request system reboot <at time> <in minutes> <media type>
<message "text">
```

Table 89 describes the `request system reboot` command options.

Table 89: CLI Request System Reboot Command Options

Option	Description
<code>none</code>	Same as <code>at now</code> (reboots the router immediately).
<code>at time</code>	Specifies the time at which to reboot the router. You can specify time in one of the following ways: <ul style="list-style-type: none"> ■ <code>now</code>—Reboots the router immediately. This is the default. ■ <code>+ minutes</code>—Reboots the router in the number of minutes from now that you specify. ■ <code>yymmddhhmm</code>—Reboots the router 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 router 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 router. 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 primary compact flash drive. This is the default. ■ <code>removable-compact-flash</code>—Reboots from the optional removable compact flash drive. This option is available on J4300 and J6300 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 router reboots.

Halting a Services Router with the CLI

You can use the `request system halt` CLI command to halt the Services Router:

```
user@host> request system halt <at time> <in minutes> <media type>
<message "text">
```

When the router is halted, all software processes stop and you can access the router through the console port only. Reboot the router by pressing any key on the keyboard.



NOTE: If you cannot connect to the router through the console port, shut down the router by pressing and holding the power button on the front panel until the POWER LED turns off. After the router has shut down, you can power on the router by pressing the power button again. The POWER LED lights during startup and remains steadily green when the router is operating normally.

Table 90 describes the request system halt command options.

Table 90: CLI Request System Halt Command Options

Option	Description
none	Same as at now (stops software processes on the router immediately).
at <i>time</i>	Time at which to stop the software processes on the router. 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 <i>minutes</i>	Specifies the number of minutes from now to stop the software processes on the router. This option is a synonym for the at +minutes option.
media <i>type</i>	Specifies the boot device to boot the router from after the halt: <ul style="list-style-type: none"> ■ compact-flash—Reboots from the primary compact flash drive. This is the default. ■ removable-compact-flash—Reboots from the optional removable compact flash drive. This option is available on J4300 and J6300 Services Routers only. ■ usb—Reboots from the USB storage device.
message " <i>text</i> "	Provides a message to display to all system users before the software processes on the router are stopped.

Chapter 9

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.

This chapter contains the following topics. For more information about system management, see the *JUNOS System Basics Configuration Guide*.

- Before You Begin on page 183
- Managing Files with the J-Web Interface on page 183
- Cleaning Up Files with the CLI on page 190
- Encrypting and Decrypting Configuration Files on page 191

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 router.

Managing Files with the J-Web Interface

This section contains the following topics:

- Cleaning Up Files on page 183
- Downloading Files on page 186
- Deleting Files on page 188

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 `/cf/var/log`—Any files that are not currently being written to are deleted.
- Deletes temporary files in `/cf/var/tmp`—Any files that have not been accessed within two days are deleted.
- Deletes all crash files in `/cf/var/crash`—Any core files that the router has written during an error are deleted.

Figure 16 shows the Clean Up Files page.

Figure 16: Clean Up Files Page

Juniper
NETWORKS

ROUTER - J4300

Monitor Configuration Diagnose **Manage** Events Logged in as: regress Help About Logout

[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	/cf/var/log	9.2M
Temporary Files	/cf/var/tmp	48K
Crash (Core) Files	/cf/var/crash	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	/cf/packages/junos-7.5R1.1-domestic
Backup JUNOS File Size	37M

[Delete backup JUNOS package](#)

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) **Juniper Your Net.**

To rotate log files and delete unnecessary files with the J-Web interface:

1. In the J-Web interface, select **Manage > Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The router rotates log files and identifies the files that can be safely deleted.

3. The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.
4. 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 17 shows the J-Web page from which you can download log files.

Figure 17: Log Files Page (Download)

Router - J4300

Monitor Configuration Diagnose **Manage** Events Logged in as: regress Help About Logout

[Manage](#) > [Files](#)

Files

Log Files

Delete...

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

Delete...

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#). [Privacy](#)

Juniper your Net.

To download files with the J-Web interface:

1. In the J-Web interface, select **Manage > 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 `/cf/var/log` directory on the router.
 - **Temporary Files**—Lists the temporary files located in the `/cf/var/tmp` directory on the router.

- **Crash (Core) Files**—Lists the core files located in the `/cf/var/crash` directory on the router.
3. The J-Web interface displays the files located in the directory.
 4. To download an individual file, click **Download**.
 5. Choose a location for the browser to save the file.
The file is saved as a text file, with a `.txt` file extension.
 6. To view the file, open it with a text editor.

Deleting Files

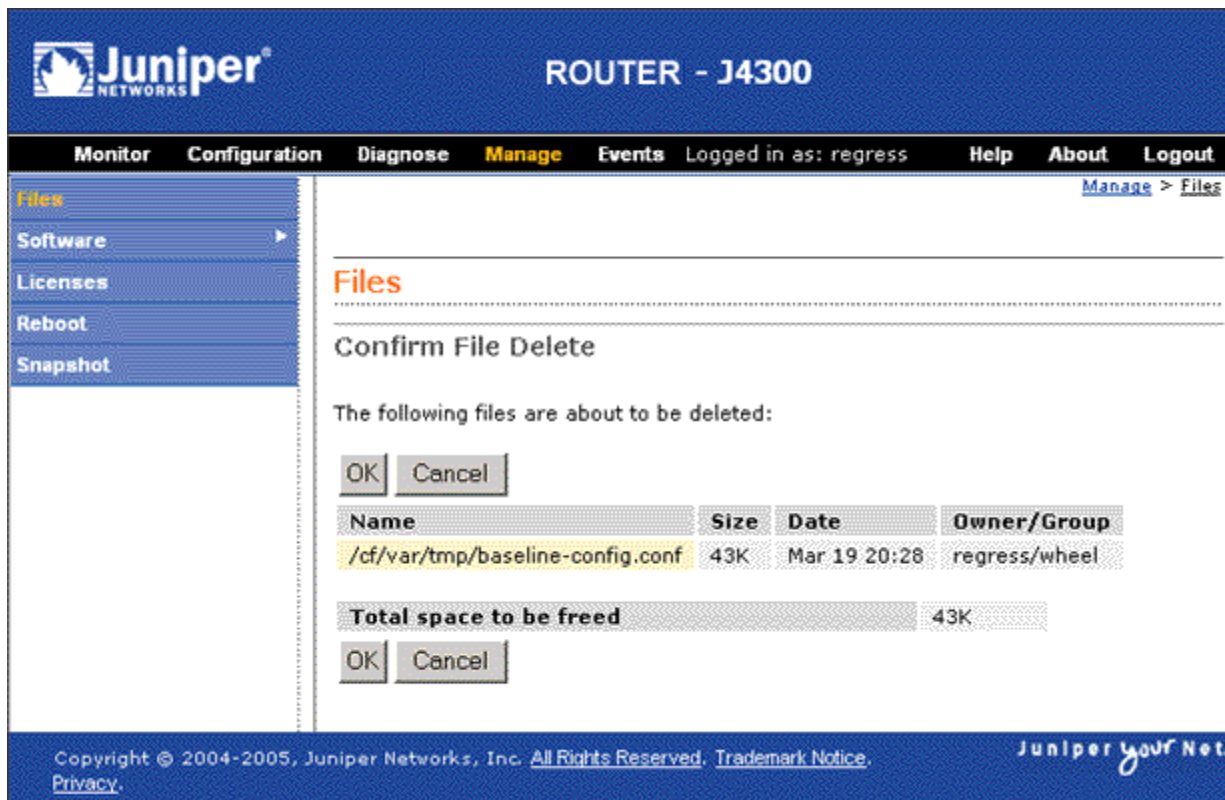
You can use the J-Web interface to delete an individual file from the Services Router. When you delete the file, it is permanently removed from the file system.



CAUTION: If you are unsure whether to delete a file from the router, we recommend using the **Cleanup Files** tool described in “Cleaning Up Files” on page 183. This tool determines which files can be safely deleted from the file system.

Figure 18 shows the J-Web page on which you confirm the deletion of files.

Figure 18: Confirm File Delete Page



To delete files with the J-Web interface:

1. In the J-Web interface, select **Manage > 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 /cf/var/log directory on the router.
 - **Temporary Files**—Lists the temporary files located in the /cf/var/tmp directory on the router.
 - **Crash (Core) Files**—Lists the core files located in the /cf/var/crash directory on the router.
3. The J-Web interface displays the files located in the directory.
4. Check the box next to each file you plan to delete.
5. 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.

6. 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**.

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, and fresh log files are created.
- Deletes log files in `/cf/var/log`—Any files that are not currently being written to are deleted.
- Deletes temporary files in `/cf/var/tmp`—Any files that have not been accessed within two days are deleted.
- Deletes all crash files in `/cf/var/crash`—Any core files that the router has written during an error 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 router 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.

Encrypting and Decrypting Configuration Files

Configuration files contain sensitive information such as IP addresses. By default, the Services Router stores configuration files in unencrypted format on a removable compact flash disk. This storage method is considered a security risk because the flash disk can easily be removed from the Services Router. To prevent unauthorized users from viewing sensitive information in configuration files, you can encrypt them.

If your router runs the Canada and U.S. version of the JUNOS Internet software, the configuration files can be encrypted with the Advanced Encryption Standard (AES) or Data Encryption Standard (DES) encryption algorithms. If your router runs the international version of the JUNOS software, the files can be encrypted only with DES.

To prevent unauthorized access, the encryption key is stored in the Services Router's EEPROM. You can copy the encrypted configuration files to another router and decrypt them if that router has the same encryption key. To prevent encrypted configuration files from being copied to another router and decrypted, you can set a unique encryption key that contains the chassis serial number of your router. Configuration files that are encrypted with a unique encryption key cannot be decrypted on any other router.

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 191
- Decrypting Configuration Files on page 193
- Modifying the Encryption Key on page 193

Encrypting Configuration Files

To encrypt configuration files on a Services Router:

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 91.

Table 91: request system set-encryption-key Commands

CLI Command	Description
request system set-encryption-key	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 the JUNOS software ■ DES encryption for the international version of the JUNOS software
request system set-encryption-key algorithm des	Sets the encryption key and specifies configuration file encryption by DES.
request system set-encryption-key unique	Sets the encryption key and enables default configuration file encryption with a unique encryption key that includes the chassis serial number of the Services Router. Configuration files encrypted with the unique key can be decrypted only on the current router. You cannot copy such configuration files to another router and decrypt them.
request system set-encryption-key des unique	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: juniper1Verifying 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 Services Router and make them readable to all:

1. Enter operational mode in the CLI.
2. To verify your permission to decrypt configuration files on this router, enter the following command and the encryption key for the router:

```
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 91. 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:juniperoneVerifying EEPROM stored
encryption key:
```

4. At the second prompt, reenter the new encryption key.

Part 4

Diagnosing Performance and Network Problems

- Using Services Router Diagnostic Tools on page 197
- Configuring Packet Capture on page 245
- Configuring RPM Probes on page 259

Chapter 10

Using Services Router Diagnostic Tools

J-series Services Routers 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.

This chapter contains the following topics. 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*.

- Diagnostic Terms on page 197
- Diagnostic Tools Overview on page 198
- Before You Begin on page 202
- Pinging Hosts from the J-Web Interface on page 203
- Checking MPLS Connections from the J-Web Interface on page 209
- Tracing Unicast Routes from the J-Web Interface on page 213
- Capturing and Viewing Packets with the J-Web Interface on page 217
- Using CLI Diagnostic Commands on page 223

Diagnostic Terms

Before diagnosing J-series Services Routers, become familiar with the terms defined in Table 92.

Table 92: J-series 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.
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.

Table 92: J-series Diagnostic Terms (continued)

Term	Definition
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 Services Router. J-Web results are displayed in the browser.

You can also diagnose the router 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 82.

- J-Web Diagnostic Tools Overview on page 198
- CLI Diagnostic Commands Overview on page 199
- MPLS Connection Checking on page 201

J-Web Diagnostic Tools Overview

The J-Web diagnostic tools consist of the options that appear when you select **Diagnose** and **Manage** in the task bar. Table 93 describes the functions of the Diagnose and Manage options.

Table 93: J-Web Interface Diagnose and Manage Options

Option	Function
Diagnose 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 204.

Table 93: 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 201.
Traceroute	Allows you to trace a route between the Services Router 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 213.
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 217.
Manage Options	
Files	Allows you manage log, temporary, and core files on the Services Router. For details, see “Managing Files with the J-Web Interface” on page 183.
Upgrade	Allows you to upgrade and manage Services Router software packages. For details, see “Performing Software Upgrades and Reboots” on page 159.
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 Getting Started Guide for your router.
Reboot	Allows you to reboot the Services Router at a specified time. For details, see “Rebooting or Halting a Services Router with the J-Web Interface” on page 177.

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. (See the Getting Started Guide for your router.)

At the top level of operational mode are the broad groups of CLI diagnostic commands listed in Table 94.

Table 94: CLI Diagnostic Command Summary

Command	Function
Controlling the CLI Environment	
<code>set option</code>	Configures the CLI display.
Diagnosis and Troubleshooting	
<code>clear</code>	Clears statistics and protocol database information.
<code>mtrace</code>	Traces information about multicast paths from source to receiver. For details, see “Tracing Multicast Routes from the CLI” on page 233.
<code>monitor</code>	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 237 ■ “Using the monitor traffic Command” on page 239 ■ “Displaying Log and Trace Files from the CLI” on page 236
<code>ping</code>	Determines the reachability of a remote network host. For details, see “Pinging Hosts from the CLI” on page 223.
<code>ping mpls</code>	Determines the reachability of an MPLS endpoint using various options. For details, see “MPLS Connection Checking” on page 201.
<code>test</code>	Tests the configuration and application of policy filters and AS path regular expressions.
<code>traceroute</code>	Traces the route to a remote network host. For details, see “Tracing Unicast Routes from the CLI” on page 229.
Connecting to Other Network Systems	
<code>ssh</code>	Opens secure shell connections. For details, see “Using the ssh Command” on page 28.
<code>telnet</code>	Opens Telnet sessions to other hosts on the network. For details, see “Using the telnet Command” on page 27.
Management	
<code>copy</code>	Copies files from one location on the Services Router to another, from the router to a remote system, or from a remote system to the router.
<code>restart option</code>	Restarts the various JUNOS software processes, including the routing protocol, interface, and SNMP processes.
<code>request</code>	Performs system-level operations, including stopping and rebooting the Services Router and loading JUNOS software images.
<code>start</code>	Exits the CLI and starts a UNIX shell.

Table 94: CLI Diagnostic Command Summary (continued)

Command	Function
configuration	Enters configuration mode. For details, see the Getting Started Guide for your router.
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 Services Router 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 Services Router receives the response packet, it reports a successful ping response.

Responses that take longer than 2 seconds are identified as failed probes.

Table 95 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 95: Options for Checking MPLS Connections

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping RSVP-signaled LSP	<code>ping mpls rsvp</code>	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The Services Router pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the Services Router sends the ping requests on the path that is currently active.
Ping LDP-signaled LSP	<code>ping mpls ldp</code>	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The Services Router pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the Services Router sends the ping requests through the first gateway. Ping requests sent to LDP-signaled LSPs use only the master routing instance.

Table 95: Options for Checking MPLS Connections (continued)

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping LSP to Layer 3 VPN prefix	ping mpls l3vpn	Checks the operability of the connections related to a Layer 3 VPN. The Services Router 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 Services Router 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 Services Router directs outgoing request probes out the specified interface.	
Instance to which this connection belongs	ping mpls l2vpn instance	Checks the operability of the connections related to a Layer 2 VPN. The Services Router 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 Services Router 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 Services Router 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 Services Router 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 203

- Ping MPLS Preparation on page 203

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 14 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 Services Router.

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 Services Router. To enable MPLS on an interface, see the *J-series Services Router Advanced WAN Access Configuration Guide*.

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 Services Router. If the outbound node is a Services Router, see the *J-series Services Router Advanced WAN Access Configuration Guide* to configure the loopback address.

Source Address for Probes

The source IP address you specify for a set of probes must be an address configured on one of the Services Router interfaces. If it is not a valid Services Router 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 204
- Ping Host Results and Output Summary on page 207

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 Services Router 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 223.)

To use the ping host tool:

1. Select **Diagnose > Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 19).
3. Enter information into the Ping Host page, as described in Table 96.

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 20). 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 97 summarizes the output fields of the display.

5. To stop the ping operation before it is complete, click **OK**.

Figure 19: Ping Host Page

Juniper NETWORKS **ROUTER - J4300**

Monitor Configuration **Diagnose** Manage Events Logged in as: regress Help About Logout

[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

Start

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved](#). [Trademark Notice](#). [Privacy](#). **Juniper your Net.**

Table 96: 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.

Table 96: J-Web Ping Host Field Summary (continued)

Field	Function	Your Action
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.
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 router 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 20: Ping Host Results Page

Juniper
NETWORKS

ROUTER - J4300

Monitor Configuration **Diagnose** Manage Events Logged in as: regress Help About Logout

[Diagnose](#) > [Ping Host](#)

Ping Host

Ping 172.17.28.19

```

PING 172.17.28.19 (172.17.28.19): 56 data bytes
64 bytes from 172.17.28.19: icmp_seq=0 ttl=55 time=254.775 ms
64 bytes from 172.17.28.19: icmp_seq=1 ttl=55 time=250.220 ms
64 bytes from 172.17.28.19: icmp_seq=2 ttl=55 time=260.243 ms
64 bytes from 172.17.28.19: icmp_seq=3 ttl=55 time=260.241 ms
64 bytes from 172.17.28.19: icmp_seq=4 ttl=55 time=260.323 ms
64 bytes from 172.17.28.19: icmp_seq=5 ttl=55 time=250.295 ms
64 bytes from 172.17.28.19: icmp_seq=6 ttl=55 time=260.455 ms
64 bytes from 172.17.28.19: icmp_seq=7 ttl=55 time=260.131 ms
64 bytes from 172.17.28.19: icmp_seq=8 ttl=55 time=260.523 ms
64 bytes from 172.17.28.19: icmp_seq=9 ttl=55 time=250.488 ms
--- 172.17.28.19 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 250.220/256.769/260.523/4.516 ms

```

OK

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) Juniper Your Net.

Ping Host Results and Output Summary

Table 97 summarizes the output in the ping host display. If the Services Router receives no ping responses from the destination host, review the list after Table 97 for a possible explanation.

Table 97: J-Web Ping Host Results and Output Summary

Field	Description
<i>bytes</i> bytes from <i>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.
icmp_seq= <i>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.
ttl= <i>number</i>	<i>number</i> —Time-to-live hop-count value of the ping response packet.
time= <i>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</i> packets transmitted	<i>number</i> —Number of ping requests (probes) sent to host.
<i>number</i> packets received	<i>number</i> —Number of ping responses received from host.
<i>percentage</i> packet loss	<i>percentage</i> —Number of ping responses divided by the number of ping requests, specified as a percentage.
round-trip min/avg/max/stddev = <i>min-time</i> / <i>avg-time</i> / <i>max-time</i> / <i>std-dev</i> ms	<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 Services Router 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 Services Router 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 223.

Before using the J-Web ping MPLS tool in your network, read “Ping MPLS Preparation” on page 203.

This section contains the following topics:

- Using the J-Web Ping MPLS Tool on page 209
- Ping MPLS Results and Output on page 212

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 Services Router.

To use the ping MPLS tool:

1. Select **Diagnose > Ping MPLS** from the task bar.
2. Next to the ping MPLS option you want to use, click the expand icon (see Figure 21).
3. Enter information into the Ping MPLS page, as described in Table 98.
4. Click **Start**.

Table 99 summarizes the output fields of the display.

5. To stop the ping operation before it is complete, click **OK**.

Figure 21: Ping MPLS Page

Juniper
NETWORKS

ROUTER - J6300

Monitor Configuration **Diagnose** Manage Events Alarms Logged in as: regress Help About Logout

Ping Host
Ping MPLS
Traceroute

[Diagnose](#) > [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

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved](#). [Trademark Notice](#). [Privacy](#). *Juniper your Net.*

Table 98: 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 Services Router 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.

Table 98: J-Web Ping MPLS Field Summary (continued)

Field	Function	Your Action
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
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 Services Router 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 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 Services Router interface.
Locate LSP using interface name		
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the Services Router 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 Services Router 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 2VPN Name	Identifies the Layer 2 VPN to ping.	Type the name of the VPN to ping.
Remote Site Identifier	Specifies the remote site identifier of the Layer 2 VPN to ping.	Type the remote site identifier for the VPN.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a Services Router 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.

Table 98: J-Web Ping MPLS Field Summary (continued)

Field	Function	Your Action
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Locate LSP from interface name		
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the Services Router 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 Services Router 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 Services Router 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 Services Router 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 99 summarizes the output in the ping MPLS display. If the Services Router receives no responses from the destination host, review the list after Table 99 for a possible explanation.

Table 99: 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 Services Router 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 Services Router 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 Services Router and a specified destination host. The output is useful for diagnosing a point of failure in the path from the Services Router to the destination host, and addressing network traffic latency and throughput problems.

The Services Router 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 214
- Traceroute Results and Output Summary on page 216

Using the J-Web Traceroute Tool

To use the traceroute tool:

1. Select **Diagnose > Traceroute**.
2. Next to Advanced options, click the expand icon (see Figure 22).
3. Enter information into the Traceroute page, as described in Table 100.

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 Services Router 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 Services Router times out before receiving a Time Exceeded message, an asterisk (*) is displayed for that round-trip time.

Table 101 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 22: Traceroute Page

Juniper
NETWORKS

ROUTER - J4300

Monitor Configuration **Diagnose** Manage Events Logged in as: regress Help About Logout

Ping Host
Ping MPLS
Traceroute

[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

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#) **Juniper Your Net.**

Table 100: 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.

Table 100: Traceroute Field Summary (continued)

Field	Function	Your Action
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.
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 router 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 101 summarizes the output in the traceroute display. If the Services Router receives no responses from the destination host, review the list after Table 101 for a possible explanation.

Table 101: 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.

Table 101: J-Web Traceroute Results and Output Summary (continued)

Field	Description
<i>time2</i>	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular 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 Services Router 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 Services Router 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 Services Router. 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 239.

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 245.

This section contains the following topics:

- Using J-Web Packet Capture on page 218
- Packet Capture Results and Output Summary on page 222

Using J-Web Packet Capture

To use J-Web packet capture:

1. Select **Diagnose > Packet Capture**.
2. Enter information into the Packet Capture page (Figure 23) as described in Table 102.

The sample configuration in Table 102 captures the next 10 TCP packets originating from the IP address 10.1.40.48 on port 23 and passing through the Fast Ethernet interface fe-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 102.

4. Click **Start**.

The captured packet headers are decoded and displayed in the Packet Capture display (see Figure 24).

Table 103 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 23: Packet Capture Page

Juniper NETWORKS ROUTER - J6300

Monitor Configuration **Diagnose** Manage Events Alarms Logged in as: regress Help About Logout

Diagnose > Packet Capture

Packet Capture

The packet capture diagnostic tool allows inspection of router control traffic (not transient traffic). The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.

Interface default **Addresses**

Add/Remove	Direction	Type	Address
Add	any	host	

Detail level brief **Protocols**

Add/Remove	Protocol
Add	tcp

Packets 10 **Ports**

Add/Remove	Direction	Port
Add	any	

Advanced options

<input type="checkbox"/> Absolute TCP Sequence	<input type="text" value="Header Expression"/>
<input type="checkbox"/> Layer 2 Headers	<input type="text" value="Packet Size"/>
<input type="checkbox"/> Non-Promiscuous	<input type="checkbox"/> Don't Resolve Addresses
<input type="checkbox"/> Display Hex	<input type="checkbox"/> No Timestamp
<input type="checkbox"/> Display ASCII and Hex	<input type="checkbox"/> Write Packet Capture File

Start

Copyright © 2004-2006, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper Your Net.

Table 102: 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, fe-0/0/0.

Table 102: Packet Capture Field Summary (continued)

Field	Function	Your Action
Detail level	<p>Specifies the extent of details to be displayed for the packet headers.</p> <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 .
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.

Table 102: Packet Capture Field Summary (continued)

Field	Function	Your Action
Non-Promiscuous	Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it.	<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.
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	Specifies the match condition for the packets to be captured. The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.	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	Writes the captured packets to a file in PCAP format in <code>/var/tmp</code> . The files are named with the prefix <code>jweb-pcap</code> and the extension <code>.pcap</code> . If you select this option, the decoded packet headers are not displayed on the packet capture page.	<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 24 shows J-Web packet capture output from router1, with the level of detail set to brief. Table 103 summarizes the output in the packet capture display.

Figure 24: Packet Capture Results Page

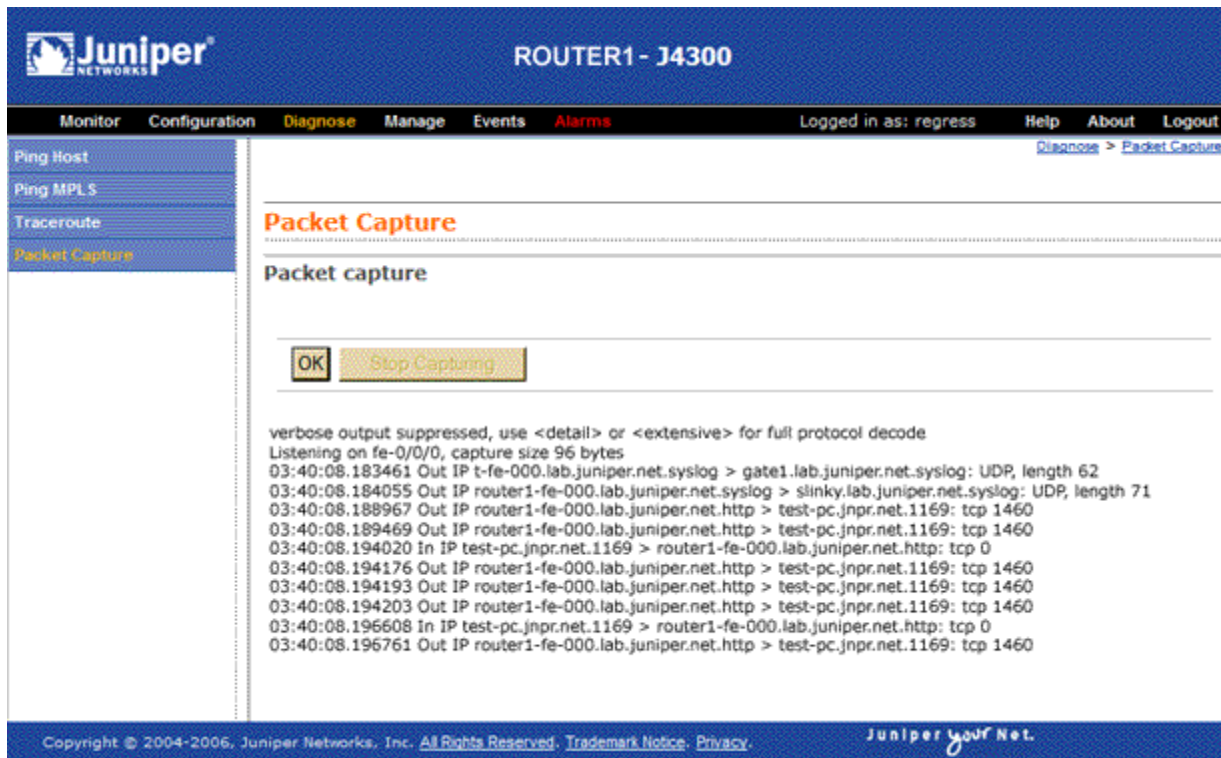


Table 103: J-Web Packet Capture Results and Output Summary

Field	Description
<i>timestamp</i>	Time when the packet was captured. The time stamp 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.

Table 103: J-Web Packet Capture Results and Output Summary (continued)

Field	Description
<i>destination address</i>	<p>Hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port are displayed.</p> <p>NOTE: When a string is defined for the port, the packet capture output displays the string instead of the port number.</p>
<i>protocol</i>	<p>Protocol for the packet.</p> <p>In the sample output, TCP indicates the Layer 4 protocol.</p>
<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 199.

This section contains the following topics:

- Pinging Hosts from the CLI on page 223
- Checking MPLS Connections from the CLI on page 225
- Tracing Unicast Routes from the CLI on page 229
- Tracing Multicast Routes from the CLI on page 233
- Displaying Log and Trace Files from the CLI on page 236
- Monitoring Interfaces and Traffic from the CLI on page 237

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 Services Router 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 204.)

Enter the `ping` command with the following syntax. Table 104 describes the `ping` command options.

```
user@host> ping host <interface source-interface> <bypass-routing>
<count number> <do-not-fragment> <inet | inet6> <interval seconds>
```

```

<logical-router logical-router-name> <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 104: CLI ping Command Options

Option	Description
<i>host</i>	Pings the hostname or IP address you specify.
interface <i>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.
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.
count <i>number</i>	(Optional) Limits the number of ping requests to send. Specify a count from 1 through 2,000,000,000. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
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 <i>seconds</i>	(Optional) Sets the interval between ping requests, in seconds. Specify an interval from 0.1 through 10,000. The default value is 1 second.
loose-source [<i>hosts</i>]	(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 <i>string</i>	(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 <i>routing-instance-name</i>	(Optional) Uses the routing instance you specify for the ping request.
size <i>bytes</i>	(Optional) Sets the size of the ping request packet. Specify a size from 0 through 65,468. The default value is 56 bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.
source <i>source-address</i>	(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 [<i>hosts</i>]	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet, and uses the list of hosts you specify for routing the packet.

Table 104: CLI ping Command Options (continued)

Option	Description
<code>tos number</code>	(Optional) Sets the type-of-service (TOS) value in the IP header of the ping request packet. Specify a value from 0 through 255.
<code>ttl number</code>	(Optional) Sets the time-to-live (TTL) value for the ping request packet. Specify a value from 0 through 255.
<code>wait seconds</code>	(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 <code>count</code> option, the Services Router uses a default count of 5 packets.
<code>detail</code>	(Optional) Displays the interface on which the ping response was received.
<code>verbose</code>	(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 207.

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 Services Router 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 Services Router 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 209.

Before using `ping mpls` commands in your network, read “Ping MPLS Preparation” on page 203.

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 226
- Pinging Layer 3 VPNs on page 227
- Pinging Layer 2 VPNs on page 227
- Pinging Layer 2 Circuits on page 229

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs

Enter the `ping mpls` command with the following syntax. Table 105 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 209.)

Table 105: 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 212.

Pinging Layer 3 VPNs

Enter the `ping mpls l3vpn` command with the following syntax. Table 106 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 209.)

Table 106: CLI ping mpls l3vpn Command Options

Option	Description
<code>l3vpn prefix prefix-name</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>l3vpn-name</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 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 l3vpn` command:

```
user@host> ping mpls l3vpn vpn1 prefix 10.255.245.122/32
!!!!!
--- lsping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

The fields in the display are the same as those displayed by the J-Web ping MPLS diagnostic tool. For information, see “Ping MPLS Results and Output” on page 212.

Pinging Layer 2 VPNs

Enter the `ping mpls l2vpn` command with the following syntax. Table 107 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 209.)

Table 107: CLI ping mpls l2vpn Command Options

Option	Description
<code>l2vpn interface interface-name</code>	Sends ping requests out the specified interface configured for the Layer 2 VPN on the outbound (egress) PE router.
<code>l2vpn instance l2vpn-instance-name local-site-id local-site-id-number remote-site-id remote-site-id-number</code>	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.
<code>bottom-label-ttl</code>	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
<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 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 212.

Pinging Layer 2 Circuits

Enter the ping mpls l2circuit command with the following syntax. Table 108 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 209.)

Table 108: CLI ping mpls l2circuit Command Options

Option	Description
l2circuit interface <i>interface-name</i>	Sends ping requests out the specified interface configured for the Layer 2 circuit on the outbound PE router.
l2circuit virtual-circuit neighbor <i>prefix-name virtual-circuit-id</i>	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.
exp <i>forwarding-class</i>	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count <i>number</i>	(Optional) Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. The default value is 5. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
source <i>source-address</i>	(Optional) Uses the source address that you specify, in the ping request packet.
detail	(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 212.

Tracing Unicast Routes from the CLI

Use the CLI traceroute command to display a list of routers between the Services Router and a specified destination host. This command is useful for diagnosing a point of failure in the path from the Services Router to the destination host, and addressing network traffic latency and throughput problems.

The Services Router 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 213.)

The `traceroute monitor` command combines ping and traceroute functionality to display real-time monitoring information about each router between the Services Router 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 230
- Using the `traceroute monitor` Command on page 231

Using the `traceroute` Command

To display a list of routers between the Services Router and a specified destination host, enter the `traceroute` command with the following syntax. Table 109 describes the `traceroute` command options.

```
user@host> traceroute host <interface interface-name>
<as-number-lookup> <bypass-routing> <gateway address> <inet
| inet6> <logical-router logical-router-name> <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 109: CLI `traceroute` Command Options

Option	Description
<code>host</code>	Sends traceroute packets to the hostname or IP address you specify.
<code>interface interface-name</code>	(Optional) Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.
<code>as-number-lookup</code>	(Optional) Displays the autonomous system (AS) number of each intermediate hop between the router and the destination host.
<code>bypass-routing</code>	(Optional) Bypasses the routing tables and sends the traceroute packets only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned. Use this option to display a route to a local system through an interface that has no route through it.
<code>gateway address</code>	(Optional) Uses the gateway you specify to route through.
<code>logical-router logical-router-name</code>	(Optional) Sends traceroute packets to this logical router.
<code>inet</code>	(Optional) Forces the traceroute packets to an IPv4 destination.
<code>inet6</code>	(Optional) Forces the traceroute packets to an IPv6 destination.

Table 109: CLI traceroute Command Options (continued)

Option	Description
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
routing-instance <i>routing-instance-name</i>	(Optional) Uses the routing instance you specify for the traceroute.
source <i>address</i>	(Optional) Uses the source address that you specify, in the traceroute packet.
tos <i>number</i>	(Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255.
ttl <i>number</i>	(Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 128.
wait <i>seconds</i>	(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 216.

Using the traceroute monitor Command

To display real-time monitoring information about each router between the Services Router and a specified destination host, enter the `traceroute monitor` command with the following syntax. Table 110 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 110: CLI traceroute monitor Command Options

Option	Description
<i>host</i>	Sends traceroute packets to the hostname or IP address you specify.
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 <code>Q</code> .
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.

Table 110: CLI traceroute monitor Command Options (continued)

Option	Description
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) Tue Jun 27 15:59:31 2006
Keys: Help Display mode Restart statistics Order of fields quit
      Packets
      Pings
Host      Loss%   Snt   Last   Avg    Best  Wrst  StDev
1. 173.24.232.66    0.0%  421    1.8    1.8    0.2   79.9    5.5
2. 173.24.232.18    0.0%  421    0.5    3.2    0.4  113.7   12.8
3. 173.26.232.22    0.0%  421    0.6    2.4    0.6   38.3    4.2
4. 173.26.232.77    0.0%  421    1.5   10.4    1.4  360.4   44.1

```

Table 111 summarizes the output fields of the display.

Table 111: CLI traceroute monitor Command Output Summary

Field	Description
host	Hostname or IP address of the Services Router issuing the traceroute monitor command.
psize <i>size</i>	Size of ping request packet, in bytes.
Keys	
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.

Table 111: CLI traceroute monitor Command Output Summary (continued)

Field	Description
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 Services Router. 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 233
- Using the `mtrace monitor` Command on page 235

Using the `mtrace from-source` Command

To display information about a multicast path from a source to the Services Router, enter the `mtrace from-source` command with the following syntax. Table 112 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 112: 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 Services Router.
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 all routers 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.
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 ) protocol ttl
```

Table 113 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 113: 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.
Round trip time <i>milliseconds</i> ms	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 Services Router 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 114 summarizes the output fields of the display.

Table 114: 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: query or response. ■ <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.
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 Services Router 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 237
- Using the monitor traffic Command on page 239

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 115 and Table 116 list the keys you use to control the display using the *interface-name* and `traffic` options. (The keys are not case sensitive.)

Table 115: 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 Services Router scrolls through the physical and logical interfaces in the same order in which they are displayed by the <code>show interfaces terse</code> command.

Table 115: CLI monitor interface Output Control Keys (continued)

Key	Action
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 116: 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 [11583]
Output bytes:                       9707279          [6542]
Input packets:                      4064553          [145]
Output packets:                      66683           [25]
Error statistics:
Input errors:                        0                [0]
Input drops:                        0                [0]
Input framing errors:                0                [0]
Carrier transitions:                 0                [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 Services Router performance. We recommend that you use filtering options—such as `count` and `matching`—to minimize the impact to packet throughput on the Services Router.

Enter the `monitor traffic` command with the following syntax. Table 117 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 217.

Table 117: 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.
<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 118 through Table 120 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.

Table 117: CLI monitor traffic Command Options (continued)

Option	Description
print-hex	(Optional) Displays each packet header, except link-layer headers, in hexadecimal format.
size <i>bytes</i>	(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 .
brief	(Optional) Displays minimum packet header information. This is the default.
detail	(Optional) Displays packet header information in moderate detail. For some protocols, you must also use the size option to see detailed information.
extensive	(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 118, enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in Table 119 (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 120 (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in Table 120.
- Binary—Expressions that use the binary operators listed in Table 120.
- Packet data accessor—Expressions that use the following syntax:

```
protocol [ byte-offset <size> ]
```

Replace *protocol* with any protocol in Table 118. 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 118: 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	
	Directional match conditions can be prepended to any Entity Type match conditions, followed by a space.
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.
Packet Length	
less <i>bytes</i>	Matches packets with lengths less than or equal to the specified value, in bytes.
greater <i>bytes</i>	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 [<i>address</i> (\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 [<i>address</i> (\icmp igrp \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.

Table 118: CLI monitor traffic Match Conditions (continued)

Match Condition	Description
tcp	Matches all TCP packets.
udp	Matches all UDP packets.

Table 119: 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 120: 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 11

Configuring Packet Capture

Packet capture is a tool that helps you to analyze network traffic and troubleshoot network problems. On a J-series Services Router, 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 217.



NOTE: J-series Services Routers can capture IPv4 packets only. 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*.

This chapter contains the following topics.

- Packet Capture Terms on page 245
- Packet Capture Overview on page 246
- Before You Begin on page 249
- Configuring Packet Capture with a Configuration Editor on page 249
- Changing Encapsulation on Interfaces with Packet Capture Configured on page 254
- Verifying Packet Capture on page 255

Packet Capture Terms

Before configuring packet capture on a Services Router, become familiar with the terms defined in Table 121.

Table 121: 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 available only on J-series routers, 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 217).
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.
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 Services Router, 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 router at the same time. Unlike traffic sampling, there are no tracing operations for packet capture.



NOTE: Enabling packet capture on the router deletes the traffic sampling configuration. Similarly, enabling traffic sampling on the router deletes the packet capture configuration.

For more information about traffic sampling, see the *JUNOS Policy Framework Configuration Guide*.

This overview contains the following topics:

- Packet Capture on Router Interfaces on page 247
- Firewall Filters for Packet Capture on page 248
- Packet Capture Files on page 248
- Analysis of Packet Capture Files on page 248

Packet Capture on Router 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 is not supported on tunnel interfaces.

Packet capture supports PPP, Cisco HDLC, Frame Relay, and other ATM encapsulations. Packet capture does not support multilink encapsulations such as multilink PPP (MLPPP).

You can capture all IPv4 packets flowing on an interface in the inbound (ingress) or outbound (egress) direction or in both directions. 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 250.



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 254.

Firewall Filters for Packet Capture

When you enable packet capture on a Services Router, 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 Services Router. 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 251.

For more information about firewall filters, see the *J-series Services Router Advanced WAN Access 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` 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 253.

For more details about analyzing packet capture files, see “Verifying Captured Packets” on page 256.

Before You Begin

Before you begin configuring packet capture, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your router.
- Configure network interfaces. See the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.
- If you do not already have an understanding of the packet capture feature, see “Packet Capture Overview” on page 246.

Configuring Packet Capture with a Configuration Editor

To configure packet capture on a Services Router, you must perform the following tasks marked *(Required)*:

- Enabling Packet Capture (Required) on page 249
- Configuring Packet Capture on an Interface (Required) on page 250
- Configuring a Firewall Filter for Packet Capture (Optional) on page 251
- Disabling Packet Capture on page 253
- Deleting Packet Capture Files on page 253

Enabling Packet Capture (Required)

To enable packet capture on the router:

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 122.
3. Go on to “Configuring Packet Capture on an Interface (Required)” on page 250.

Table 122: 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 Configuration > View and Edit > Edit Configuration. 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>	From the [edit] hierarchy level, enter edit forwarding-options
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. 	Enter set packet-capture maximum-capture-size 500
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 .	In the Filename box, type pcap-file .	Enter set packet-capture file filename pcap-file
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.	Enter set packet-capture file files 100
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.	Enter set packet-capture file size 1024
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. 	Enter set packet-capture file world-readable

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 123.
3. If you are finished configuring the router, 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 251.
 - To check the configuration, see “Verifying Packet Capture” on page 255.

Table 123: 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.	<ol style="list-style-type: none"> 1. In the J-Web interface, select Configuration > View and Edit > Edit Configuration. 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.	<ol 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: Packets originating from the host router 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 124.

3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying Packet Capture” on page 255.

Table 124: 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 Configuration > View and Edit > Edit Configuration. 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 .	<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 125.
3. If you are finished configuring the router, commit the configuration.

Table 125: Disabling 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 Configuration > View and Edit > Edit Configuration. 2. Next to Forwarding options, click Configure or Edit. 	From the [edit] hierarchy level, enter edit forwarding-options
Disable packet capture.	<ol 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 set packet-capture disable.

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 253.
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 249.
4. Commit the configuration.

Changing Encapsulation on Interfaces with Packet Capture Configured

Before modifying the encapsulation on a Services Router 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 253.
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 *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

5. Commit the configuration.
6. Reenable packet capture following the steps in “Enabling Packet Capture (Required)” on page 249.
7. Commit the configuration.

Verifying Packet Capture

To verify packet capture, perform these tasks:

- Displaying a Packet Capture Configuration on page 255
- Displaying a Firewall Filter for Packet Capture Configuration on page 256
- Verifying Captured Packets on page 256

Displaying a Packet Capture Configuration

Purpose	Verify the packet capture configuration.
Action	From the J-Web interface, select Configuration > View and Edit > View Configuration Text . Alternatively, from configuration mode in the CLI, enter the show forwarding-options command.
Sample Output	<pre>[edit] user@host# show forwarding-options packet-capture { file filename pcap-file files 100 size 1024;</pre>

```

        maximum-capture-size 500;
    }

```

What It Means Verify that the output shows the intended file configuration for capturing packets. For more information about the format of a configuration file, see the information about viewing configuration text in the *J-series Services Router Basic LAN and WAN Access Configuration 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 **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the `show firewall filter dest-all` command.

Sample Output

```

[edit]
user@host# show firewall filter dest-all
term dest-term {
    from {
        destination-address 192.168.1.1/32;
    }
    then {
        sample;
        accept;
    }
}

```

What It Means 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. For more information about the format of a configuration file, see the information about viewing configuration text in the *J-series Services Router Basic LAN and WAN Access Configuration 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 253.
- 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 router:

```
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 -xvvvvv
```

```
01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800), length 98:
    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:
    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%
```

What It Means

Verify that the output shows the intended packets.

Chapter 12

Configuring RPM Probes

J-series Services Routers support a tool that allows network operators and their customers to accurately measure the performance between two network endpoints. With the real-time performance monitoring (RPM) feature, you configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter.

This chapter contains the following topics. For more information about RPM, see the *JUNOS Services Interfaces Configuration Guide*.

- RPM Terms on page 259
- RPM Overview on page 260
- Before You Begin on page 263
- Configuring RPM with Quick Configuration on page 263
- Configuring RPM with a Configuration Editor on page 270
- Verifying an RPM Configuration on page 280

RPM Terms

Before configuring and monitoring RPM on J-series Services Routers, become familiar with the terms defined in Table 126.

Table 126: RPM Terms

Term	Definition
egress	Outbound. Characterizing packets exiting a Services Router.
ingress	Inbound. Characterizing packets entering a Services Router.
jitter	Variation in the rate at which packets in a stream are received, 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.
probe interval	Time, in seconds, between probe packets.

Table 126: RPM Terms (continued)

Term	Definition
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 Services Router 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 Services Router, the router 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 260
- RPM Tests on page 261
- Probe and Test Intervals on page 261
- RPM Statistics on page 261
- RPM Thresholds and Traps on page 262
- RPM for BGP Monitoring on page 262

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 Services Router. By analyzing the transit times to and from the remote server, the Services Router can determine network performance statistics.

The Services Router 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.

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 have 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.

RPM Statistics

At the end of each test, the Services Router collects the statistics for packet round-trip time, packet inbound and outbound times (for ICMP timestamp probes only), and probe loss shown in Table 127.

Table 127: RPM Statistics

RPM Statistics	Description
Round-Trip Times	
Minimum round-trip time	Shortest round-trip time from the Services Router to the remote server, as measured over the course of the test
Maximum round-trip time	Longest round-trip time from the Services Router to the remote server, as measured over the course of the test
Average round-trip time	Average round-trip time from the Services Router 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 Services Router to the remote server, as measured over the course of the test

Table 127: RPM Statistics (continued)

RPM Statistics	Description
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 Services Router 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 Services Router, as measured over the course of the test
Average egress time	Average one-way time from the Services Router 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 Services Router, as measured over the course of the test
Standard deviation egress time	Standard deviation of the one-way times from the Services Router 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 Services Router, as measured over the course of the test
Egress jitter	Difference between the maximum and minimum outbound times, as measured over the course of the test
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
Probe Counts	
Probes sent	Total number of probes sent over the course of the test
Probe responses received	Total number of probe responses received over the course of the test
Loss percentage	Percentage of probes sent for which a response was not received

RPM Thresholds and Traps

You can configure RPM threshold values for the round-trip times, ingress (inbound) times, and egress (outbound) times that are measured for each probe, as well as for the standard deviation and jitter values that are measured for each test. Additionally, you can configure threshold values for the number of successive lost probes within a test and the total number of lost probes within a test.

If the result of a probe or test exceeds any threshold, the Services Router 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 Services Router 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 Services Router has a large number of BGP neighbors configured.

In the Services Router, you can configure RPM probes to monitor the BGP neighbors and determine if they are active.

For BGP configuration information, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Before You Begin

Before you begin configuring RPM, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your router.
- Configure network interfaces. See the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.
- Configure SNMP. See “Configuring SNMP for Network Management” on page 31.

Configuring RPM with Quick Configuration

J-Web Quick Configuration allows you to configure real-time performance monitoring (RPM) parameters. Figure 25 shows the main Quick Configuration page for RPM. Figure 26 shows the probe test Quick Configuration page for RPM.

Figure 25: Main Quick Configuration Page for RPM

Juniper
NETWORKS

ROUTER - J4300

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

[Quick Configuration](#) [View and Edit](#) [History](#) [Rescue](#)

[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 ?

Copyright © 2004-2005, Juniper Networks, Inc. [All Rights Reserved](#). [Trademark Notice](#). [Privacy](#).

Juniper your Net.

Figure 26: Probe Test Quick Configuration Page for RPM

Juniper
NETWORKS

ROUTER - J4300

Monitor **Configuration** Diagnose Manage Events Logged in as: regress Help About Logout

[Configuration](#) > [Quick Configuration](#) > [Realtime Performance Monitoring](#)

Quick Configuration

Realtime Performance Monitoring [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 ?

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 **Configuration > Quick Configuration > Realtime Performance Monitoring**.
2. Enter information into the Quick Configuration page for RPM, as described in Table 128.
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 280.

Table 128: 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 http:// .
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 router'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 icmp and icmp-timestamp . The default routing instance is inet.0 .
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		

Table 128: RPM Quick Configuration Summary (continued)

Field	Function	Your Action
Probe Type (required)	Specifies the type of probe to send as part of the test.	<p>Select the desired probe type from the list:</p> <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.
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 (Services Router) and the remote server must be Juniper Networks routers 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>J-series Services Router Advanced WAN Access 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.
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.

Table 128: RPM Quick Configuration Summary (continued)

Field	Function	Your Action
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 Services Router to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter	Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Sets the total one-way time (in microseconds), from the Services Router 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 Services Router, 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		

Table 128: RPM Quick Configuration Summary (continued)

Field	Function	Your Action
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.
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.

Table 128: RPM Quick Configuration Summary (continued)

Field	Function	Your Action
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 Services Router is to receive and transmit TCP probes.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
UDP Probe Server	Specifies the port on which the Services Router is to receive and transmit UDP probes.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.

Configuring RPM with a Configuration Editor

To configure the Services Router to perform real-time performance tests, you perform the following tasks. For information about using the J-Web and CLI configuration editors, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

- Configuring Basic RPM Probes on page 270
- Configuring TCP and UDP Probes on page 274
- Tuning RPM Probes on page 276
- Configuring RPM Probes to Monitor BGP Neighbors on page 277

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.

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 129.
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 274.
 - To tune a probe, see “Tuning RPM Probes” on page 276.
 - To check the configuration, see “Verifying an RPM Configuration” on page 280.

Table 129: 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 Configuration > View and Edit > Edit Configuration.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 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 above steps and add an RPM probe owner for customerB.	<ol style="list-style-type: none">1. Enter set probe customerA2. Enter set probe customerB

Table 129: Configuring Basic RPM Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the RPM test icmp-test for the RPM owner customerA .	1. On the Rpm page, select customerA .	1. From the [edit] hierarchy level, enter
The sample RPM test is an ICMP probe with a test interval (probe frequency) of 15 seconds, a probe type of icmp-ping-timestamp , and a target address of 192.178.16.5 .	2. In the Test box, click Add new entry	edit services rpm probe customerA
	3. In the Name box, type icmp-test .	2. Enter
	4. In the Test interval box, type 15 .	set test icmp-test probe-frequency 15
	5. In the Probe type box, select icmp-ping-timestamp .	3. Enter
	6. In the Target box, select the Yes check box, and click Configure .	set test icmp-test probe-type icmp-ping-timestamp
	7. In the Target type box, select Address .	4. Enter
	8. In the Address box, type 192.178.16.5 .	set test icmp-test target address 192.178.16.5
	9. Click OK .	
Configure RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.	1. On the Probe page, select icmp-test .	1. Enter
	2. In the Thresholds box, select the Yes check box, and click Configure .	set probe customerA test icmp-test thresholds ingress-time 3000
	3. In the Ingress time box, type 3000 .	2. Enter
	4. Click OK .	set probe customerA test icmp-test traps ingress-time-exceeded
	5. In the Traps box, click Add new entry .	
	6. In the Value box, select ingress-time-exceeded .	
	7. Click OK .	

Table 129: Configuring Basic RPM Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
<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
<p>Configure RPM thresholds and corresponding SNMP traps to catch 3 or more successive lost probes and total lost probes of 10 or more.</p>	<ol style="list-style-type: none"> 1. On the Probe page, select http-test. 2. In the Thresholds box, select the Yes check box, and click Configure. 3. In the Successive loss box, type 3. 4. In the Total loss box, type 10. 5. Click OK. 6. In the Traps box, click Add new entry. 7. In the Value box, select probe-failure. 8. Click OK. 9. In the Traps box, click Add new entry. 10. In the Value box, select test-failure. 11. Click OK. 	<ol style="list-style-type: none"> 1. Enter set probe customerB test icmp-test thresholds successive-loss 3 2. Enter set probe customerB test icmp-test thresholds total-loss 10 3. Enter set probe customerB test icmp-test traps probe-failure 4. Enter set probe customerB test icmp-test traps test-failure

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 Services Router and the remote Services Router to act as TCP and UDP servers.

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 router is configured as an RPM server for both TCP and UDP packets, using ports 50000 and 50037, respectively. Router A is the host router in this example, and Router B is the remote router. 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 130.
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 276.
 - To check the configuration, see “Verifying an RPM Configuration” on page 280.

Table 130: 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 Configuration > View and Edit > Edit Configuration. 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 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. 	Enter set probe customerC

Table 130: Configuring TCP and UDP Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
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
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 Configuration > View and Edit > Edit Configuration. 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 270.

To configure tune RPM probes:

1. Perform the configuration tasks described in Table 129.
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 131.
4. If you are finished configuring the network, commit the configuration.
5. To check the configuration, see “Verifying an RPM Configuration” on page 280.

Table 131: 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 Configuration > View and Edit > Edit Configuration. 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

Table 131: Tuning RPM Probes (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
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.	1. In the Source address box, type 192.168.2.9.	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.	2. Click OK .	

Configuring RPM Probes to Monitor BGP Neighbors

By default, the Services Router 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 277
- Directing RPM Probes to Select BGP Routers on page 279

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 (Services Router) and the probe receiver (the remote Services Router) 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 Services Router 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 132.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following tasks:
 - To send probes to specific routers, see “Directing RPM Probes to Select BGP Routers” on page 279.

- To check the configuration, see “Verifying an RPM Configuration” on page 280.

Table 132: 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 Configuration > View and Edit > Edit Configuration. 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
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"> 1. In the Probe count box, type 5. 2. 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"> 1. In the Test interval box, type 60. 2. Click OK. 	Enter set test-interval 60

Directing RPM Probes to Select BGP Routers

If a Services Router 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 or a combination of logical routers and routing instances.

The sample RPM configuration in Table 133 sends RPM probes to the BGP neighbors in the following logical routers or logical router-routing instance combinations:

- Default logical router and default routing instance
- Logical router LR1
- Routing instance RI1
- Routing instance RI2 in the logical router LR1

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 133.
3. If you are finished configuring the router, commit the configuration.
4. To verify the configuration, see “Verifying an RPM Configuration” on page 280.

Table 133: 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.	1. In the J-Web interface, select Configuration > View and Edit > Edit Configuration .	From the [edit] hierarchy level, enter
	2. Next to Services, click Configure or Edit .	edit services rpm bgp
	3. Next to Rpm, select the Yes check box and click Configure or Edit .	
	4. Next to Bgp, click Configure or Edit .	

Table 133: Directing RPM Probes to Select BGP Routers (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the default logical router and default routing instance.	<ol style="list-style-type: none"> 1. Next to Logical router, click Add new entry. 2. In the Logical router name box, type default. 3. Next to Routing instances, click Add new entry. 4. In the Routing instance name box, type null. 5. Click OK until you return to the RPM page. 	<p>Enter</p> <p>set logical-router default routing-instance null</p>
Configure logical router LR1 to send RPM probes to BGP neighbors within the logical router.	<ol style="list-style-type: none"> 1. Next to Logical router, click Add new entry. 2. In the Logical router name box, type LR1. 3. Click OK. 	<p>Enter</p> <p>set logical-router LR1</p>
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. 	<p>Enter</p> <p>set routing-instances RI1</p>
Configure routing instance RI2 under the logical router LR1 if you want to send RPM probes to the BGP neighbors within the routing instance in the logical router.	<ol style="list-style-type: none"> 1. In the Logical router name box, click LR1. 2. Next to Routing instances, click Add new entry. 3. In the Routing instance name box, type RI2. 4. Click OK. 	<p>Enter</p> <p>set logical-router LR1 routing-instance RI2</p>

Verifying an RPM Configuration

To verify an RPM configuration, perform these tasks:

- Verifying RPM Statistics on page 281
- Verifying RPM Probe Servers on page 282

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 Monitor > RPM . From the CLI, enter the <code>show services rpm probe-results</code> command.
Sample Output	<pre> 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 </pre>
What It Means	<p>The output shows the probe results for the RPM tests configured on the Services Router. Verify the following information:</p> <ul style="list-style-type: none"> ■ 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 performance 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).

For more information about `show services rpm probe-results`, see the *JUNOS System Basics and Services Command Reference*.

Verifying RPM Probe Servers

Purpose	Verify that the Services Router is configured to receive and transmit TCP and UDP RPM probes on the correct ports.
Action	From the CLI, enter the <code>show services rpm active-servers</code> command.
Sample Output	<pre>user@host> show services rpm active-servers Protocol: TCP, Port: 50000 Protocol: UDP, Port: 50037</pre>
What It Means	<p>The output shows a list of the protocols and corresponding ports for which the Services Router is configured as an RPM server.</p> <p>For more information about <code>show services rpm active-servers</code>, see the <i>JUNOS System Basics and Services Command Reference</i>.</p>

Part 5

Index

Index

Symbols

[], in configuration statements	xvii
{ }, in configuration statements	xvii
(), in syntax descriptions	xvii
< >, in syntax descriptions	xvii
(pipe) command	82
(pipe), in syntax descriptions	xvii
#, comments in configuration statements	xvii

A

access privileges	
denying and allowing commands	7
permission bits for	5
predefined	7
specifying (Quick Configuration)	15
accounts <i>See</i> template accounts; user accounts	
activate system scripts commit command	68
activate system scripts op command	70
active alarms <i>See</i> alarms, active	
active routes, displaying	92
adapters, for compact flash recovery	175
adaptive services module, alarm conditions and	
configuration options	146
Add a RADIUS Server page	9
field summary	10
Add a TACACS+ Server page	11
field summary	12
Add a User Quick Configuration page	15
field summary	16
addresses	
attacking, displaying with IDS	115
destination, displaying	92
under attack, displaying with IDS	115
Advanced Encryption Standard (AES) <i>See</i> AES encryption	
AES encryption	
for Canada and U.S JUNOS	191
setting	192
agents, SNMP <i>See</i> SNMP agents	
alarm class <i>See</i> alarm severity	
ALARM LED, color	144
alarm severity	145
action required	154
configuring for an interface	150

displaying	154
major (red)	145
minor (yellow)	145
<i>See also</i> major alarms; minor alarms	
alarms	
active, checking	152
active, displaying at login	152
conditions, in chassis components	149
conditions, on an interface	146
configurable	146
configuration requirements for interface	
alarms	150
displaying for chassis	88
displaying for interfaces	90
licenses	149
major <i>See</i> major alarms	
minor <i>See</i> minor alarms	
monitoring	152
overview	144
red <i>See</i> major alarms	
red J-Web indicator	152
rescue configuration	149
severity <i>See</i> alarm severity	
types	144
verifying	154
yellow <i>See</i> minor alarms	
Alarms Summary page	153
alert logging severity	132
alias, CoS value	101
alternative boot media <i>See</i> boot devices; USB	
ambient temperature	88
any level statement	136
any logging facility	132
archiving system logs	136
arithmetic operators, for multicast traffic	242
AS path, displaying	92
attacks, detecting with IDS	114
authentication	
adding a RADIUS server (Quick Configuration)	8
adding a TACACS+ server (Quick Configuration)	10
local password, by default	12
login classes	5, 21
methods	4–5

order of user authentication (configuration editor).....	19
RADIUS authentication (configuration editor).....	17
specifying a method (Quick Configuration)	14
specifying access privileges (Quick Configuration)	15
TACACS + authentication (configuration editor).....	18
user accounts	4, 23
authorization logging facility	132
autoinstallation, compatibility with the DHCP server	49

B

BGP (Border Gateway Protocol)	
monitoring	93
peers, probes to <i>See</i> BGP RPM probes	
RPM probes to BGP neighbors <i>See</i> BGP RPM probes	
statistics	93
status	93
BGP groups, displaying	93
BGP neighbors	
directing RPM probes to	279
displaying	93
monitoring with RPM probes	277
BGP peers <i>See</i> BGP neighbors	
BGP routing information	93
BGP RPM probes	
directing to select BGP neighbors (configuration editor).....	279
overview	262
setting up on local and remote Services Router (configuration editor)	277
BGP sessions, status	94
binary operators, for multicast traffic	242
boot devices	167
configuring (CLI)	171
configuring (J-Web)	168
selecting (CLI)	180–181
selecting (J-Web)	179
storing memory snapshots	173
<i>See also</i> compact flash; USB	
boot operations, DHCP	56
braces, in configuration statements	xvii
brackets	
angle, in syntax descriptions	xvii
square, in configuration statements	xvii
brute force attacks, preventing	29
bytes transmitted	90

C

capturing packets <i>See</i> packet capture	
/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	
change-log logging facility	132

chassis	
alarm condition indicator	154
alarm conditions and remedies	149
alarms, displaying	88
component part numbers	89
component serial numbers	89
environment, displaying	88
identifiers, displaying	88
monitoring	87
temperature, displaying	88
circuits, DLSw	97
classifiers, CoS	100
Clean Up Files page	185
cleaning up files	183, 190
clear system services dhcp binding command	61
clear system services dhcp conflicts command	49
CLI configuration editor	
controlling user access	21
DHCP server	56
enabling commit scripts	66
enabling operation scripts	69
event policies	72
interface alarms	150
RADIUS authentication	17
RPM	270
SNMP	39
system log messages, sending to a file	134
system log messages, sending to a terminal	135
TACACS + authentication	18
code point aliases, CoS	101
comments, in configuration statements	xvii
commit scripts	
disabling	67
enabling	66
overview	65
superuser privileges required for	66
/var/db/scripts/commit directory	66
communities, SNMP <i>See</i> SNMP communities	
compact flash	173
configuring	172
configuring for failure snapshot storage	173
displaying size	86
displaying usage	87
minor (yellow) alarm	149
primary, recovering	173
recovering	173
<i>See also</i> compact flash recovery	
compact flash recovery	
adapter for	175
copying the JUNOS image	175
reasons for	174
requirements	174
components	
part numbers	89
serial numbers	89

- /config directory
 - file encryption *See* file encryption
 - snapshots for boot directories (CLI) 172
 - snapshots for boot directories (J-Web) 171
- configuration
 - alarm condition indicator 154
 - consistency checking, with commit scripts 65
 - downgrading software (CLI) 167
 - downgrading software (J-Web) 167
 - interfaces, displaying 90
 - modification and checking with operation
 - scripts 68
 - rule enforcement, with commit scripts 65
 - upgrading (CLI) 166
 - upgrading (J-Web) 163
- configuration database, displaying size 87
- configuration files
 - decrypting 183
 - encrypting 183
- configuration management, automating 65
 - See also* commit scripts; operation scripts
- configuring
 - password retry limits 30
- Confirm File Delete page 189
- console port
 - disabling 27
 - securing 26
- controlling user access 21
- conventions
 - notice icons xvi
 - text and syntax xvi
- CoS (class of service)
 - classifiers 100
 - CoS value aliases 101
 - forwarding classes 102
 - interfaces 99
 - loss priority 106
 - packet loss priority 106
 - RED drop profiles 101
 - rewrite rules 103
 - scheduler maps 104
- CPU usage, displaying 86
- crash files
 - cleaning up (CLI) 190
 - cleaning up (J-Web) 185
 - displaying size 87
 - downloading (J-Web) 187
- critical logging severity 132
- cron logging facility 132
- curly braces, in configuration statements xvii
- customer support xx
 - contacting JTAC xx
 - hardware information for 88
- Cygwin, for compact flash recovery 175

D

- daemon logging facility 132
- Data Encryption Standard (DES) *See* DES encryption
- dd utility, for compact flash recovery 175
- deactivate system scripts commit command 67
- deactivate system scripts op command 70
- debug logging severity 132
- decryption, configuration files *See* file encryption
- delete system scripts commit command 67
- delete system scripts op command 70
- deleting
 - crash files (CLI) 190
 - crash files (J-Web) 185
 - files, with caution 188
 - log files (CLI) 190
 - log files (J-Web) 185
 - temporary files (CLI) 190
 - temporary files (J-Web) 185
- DES encryption
 - for international JUNOS 191
 - setting 192
- destination address, displaying 92
- DHCP (Dynamic Host Configuration Protocol) 48
 - autoinstallation, compatibility with 49
 - configuring the server (configuration editor) 56
 - conflict detection and resolution 49
 - conflicts 119
 - interface restrictions 49
 - monitoring 118
 - options 49
 - overview 48
 - Quick Configuration 50
 - server function 47
 - verification 59
 - See also* DHCP server
- DHCP binding database, verifying 60
- DHCP leases
 - configuring (Quick Configuration) 55
 - monitoring 119
- DHCP pages
 - field summary 54
 - main 51
 - pool information 52
 - static binding page 53
- DHCP pools
 - configuring (Quick Configuration) 54
 - monitoring 119
- DHCP server
 - boot operations (Quick Configuration) 56
 - configuring (configuration editor) 56
 - displaying configurations 60
 - information (Quick Configuration) 55
 - monitoring operations 119
 - preparation 50
 - Quick Configuration 50

sample configuration	57	system logs	136
static bindings (Quick Configuration)	56	discarded packets	91
statistics	63	disconnection of console cable for console logout	27
subnet and single client	58	DLSw (data link switching)	
subnet for configuration (Quick Configuration)	54	circuits	97
verifying a configuration	60	initial pacing window	97
verifying operation	62	monitoring	97
verifying the DHCP binding database	60	peer information	98
diagnosis		peer IP address	97
alarm configurations	154	protocol version	97
automating with event policies	71	reachability	98
<i>See also</i> event policies		software version	97
chassis	149	vendor ID	97
CLI command summary	199	DLSw routing information	97
DHCP conflicts	119	DNS (Domain Name System) server address,	
DHCP statistics	63	displaying	85
displaying DHCP server configurations	60	documentation set	
displaying firewall filter for	256	comments on	xx
displaying packet capture configurations	255	Domain Name System address, displaying	85
hardware	149	downgrading	
interfaces	146, 237	software, with J-Web	167
J-Web tools overview	198	software, with the CLI	167
license infringement	149	download URL	162
monitoring network performance	259	downloading	
MPLS connections (J-Web)	209	crash files (J-Web)	187
multicast paths	233	log files (J-Web)	187
network traffic	239	software upgrades	162
packet capture	245	temporary files (J-Web)	187
packet capture (J-Web)	217	drop probabilities, CoS	101
ping command	223	drop profiles, CoS	101
ping host (J-Web)	204	dropped packets	91
ping MPLS (J-Web)	209	DS1 ports <i>See</i> T1 ports	
ports	146	DS3 ports <i>See</i> E3 ports; T3 ports	
preparation	83, 202	DSCPs (DiffServ code points)	
system logs	129	bits for RPM probes	267
system operation	236	dynamic binding, DHCP <i>See</i> DHCP; DHCP leases;	
traceroute (J-Web)	213	DHCP server	
traceroute command	229	Dynamic Host Configuration Protocol <i>See</i> DHCP	
traceroute monitor command	229		
traffic analysis with packet capture	245	E	
verifying captured packets	256	E3 ports, alarm conditions and configuration	
verifying DHCP binding database	60	options	147
verifying DHCP server operation	62	egress <i>See</i> RPM probes, outbound times	
verifying RPM probe servers	282	emergency logging severity	132
verifying RPM statistics	281	encapsulation, modifying on packet capture-enabled	
viewing active alarms	153	interfaces	254
diagnostic commands	199	encryption, configuration files <i>See</i> file encryption	
dictionary attacks, preventing	29	enforcement of configuration rules	65
DiffServ code points, bits for RPM probes	267	error logging severity	132
disabling		event notifications, automating response to with event	
commit scripts	67	policies	71
console port	27	<i>See also</i> SNMP traps; system log messages	
operation scripts	70	event policies	
packet capture	253	configuration editor	72
root login to console port	27	overview	71

event viewer, J-Web 137
See also system log messages
 Extensible Stylesheet Language Transformations
 (XSLT) *See* commit scripts; operation scripts

F

facility none statement 136
 failures
 PIM 149
 Routing Engine fan 149
 fan 88
 Fast Ethernet ports
 alarm condition indicator 154
 alarm conditions and configuration options 146
 configuring alarms on 150
 file encryption
 decrypting configuration files 193
 directories 191
 encrypting configuration files 191
 encryption algorithms required for JUNOS
 versions 191
 encryption key 191
 .gz.jc file extension 191
 overview 191
 superuser privileges required for 191
 file management
 configuration files 183
 crash files (CLI) 190
 crash files (J-Web) 183
 encryption-decryption *See* file encryption
 log files 183
 log files (CLI) 190
 log files (J-Web) 183
 packet capture file creation 248
 temporary files (CLI) 190
 temporary files (J-Web) 183
 filtering
 command output 82
 system log messages 138
 system log messages, regular expressions for ... 132
 filters *See* firewall filters; stateful firewall filters
 firewall filters
 for packet capture, configuring 251
 for packet capture, overview 248
 stateful *See* stateful firewall filters
 firewalls *See* firewall filters; stateful firewall filters
 flapping 90
 font conventions xvi
 forwarding classes, CoS 102
 FPC, PIM slot number in command displays 88
 framing errors 91
 frequency, test *See* RPM probes, test intervals

G

get requests 32

glossary
 alarms 143
 DHCP 47
 diagnostic 197
 monitoring 77
 packet capture 245
 RPM 259
 system logs 129
 user authentication 3
 groups
 BGP, displaying 93
 for SNMP traps 41
 .gz.jc file extension *See* file encryption
 gzip utility, for compact flash recovery 175

H

halting a Services Router
 with J-Web 177
 with the CLI 180
 halting a Services Router immediately
 with J-Web 179
 with the CLI 181
 hardware
 alarm conditions and remedies 149
 version, displaying 89
 health monitor *See* SNMP health monitor
 help syslog ? command 71
 host reachability
 ping command 223
 ping host (J-Web) 204
 hostname
 displaying (J-Web) 85
 monitoring traffic by matching 241
 opening an SSH session to 28
 overriding for SNMP (configuration editor) 40
 overriding for SNMP (Quick Configuration) 36
 pinging (CLI) 224
 pinging (J-Web) 205
 resolving 57
 SNMP trap target (Quick Configuration) 37
 telnetting to 28
 tracing a route to (CLI) 230–231
 tracing a route to (J-Web) 215
 HTTP (Hypertext Transfer Protocol), RPM probes 260
 Hypertext Transfer Protocol, RPM probes 260

I

ICMP (Internet Control Message Protocol)
 RPM probes, description 260
 RPM probes, inbound and outbound times 262
 RPM probes, setting 270
 idle time, displaying 85
 IDS (intrusion detection service)
 information, displaying 115
 monitoring 114

search-narrowing characteristics	115
IKE security associations, monitoring	117
inbound time <i>See</i> RPM probes	
info logging severity	132
ingress <i>See</i> RPM probes, inbound times	
initial pacing window, DLSw	97
Install Remote page	163
field summary	164, 170
installation	
software upgrades (CLI)	166
software upgrades, from a remote server	163
software upgrades, uploading	164
Instance to which this connection belongs	
description	202
using	211
interactive-commands logging facility	132
interfaces <i>See</i> management interfaces; network interfaces; ports	
Internet Key Exchange (IKE) security associations, monitoring	117
intervals, probe and test <i>See</i> RPM probes	
intrusion detection service <i>See</i> IDS	
ipconfig command	62
explanation	63
IPSec (IP Security)	
monitoring	116
statistics	116
tunnels, displaying	116

J

J-series

alarms	143
automating operations with scripts	65
automating troubleshooting with scripts and event policies	65
DHCP server	47
diagnosis	197
managing access	3
managing files	183
managing user authentication	3
monitoring	77
network management	31
packet capture	245
performance monitoring	259
release notes, URL	xv
software upgrades	159
system log messages	129
J-Web configuration editor	
controlling user access	21
DHCP server	56
enabling commit scripts	66
enabling operation scripts	69
event policies	72
interface alarms	150
RADIUS authentication	17

RPM	270
SNMP	39
system log messages, sending to a file	134
system log messages, sending to a terminal	135
TACACS + authentication	18
J-Web interface	
Diagnose options	198
event viewer	137
managing files	183
Monitor options	78
jitter	
description	262
<i>See also</i> RPM probes	
monitoring	123
threshold, setting	268
JTAC (Juniper Networks Technical Assistance Center)	
hardware information for	88
JUNOS CLI	
access privilege levels	6
automatic command execution with event policies	71
denying and allowing commands	7
diagnostic command summary	200
filtering command output	82
monitoring (show) commands summary	78
JUNOS Internet software	
encryption <i>See</i> file encryption	
known problems, operation scripts as workarounds	68
release notes, URL	xv
upgrading	159
version, displaying	85
junos-jseries package <i>See</i> upgrades	
JUNOScript Extensible Markup Language (XML)	
<i>See</i> commit scripts; operation scripts	

K

kernel logging facility	132
-------------------------	-----

L

label-switched paths <i>See</i> LSPs	
Layer 2 circuits, monitoring	209
Layer 2 VPNs, monitoring	209
Layer 3 VPNs, monitoring	209
libpcap format, for packet capture files	257
license infringement, alarm condition indicator	154
licenses, alarm conditions and remedies	149
link states, displaying	89
local password	
default authentication method	12
order of user authentication (configuration editor)	20
specifying for authentication (Quick Configuration)	14
local template accounts	25

Locate LSP from interface name	
description	202
using	212
Locate LSP from virtual circuit information	
description	202
using	212
Locate LSP using interface name	
description	202
using	211
log files	
archiving	183
deleting unused files	183
rotating	183
Log Files page (Download)	187
log messages <i>See</i> system log messages	
logging facilities	132
logging severity levels	132
logical interfaces, CoS	99
logical operators, for multicast traffic	242
login classes	
defining (configuration editor)	22
permission bits for	6
predefined permissions	7
specifying (Quick Configuration)	15
login retry limits, setting	29
login time, displaying	85
logs <i>See</i> system logs	
loopback address, displaying	85
loss priority, CoS	106
LSPs (label-switched paths)	
information about	107
monitoring, with ping MPLS	209
statistics	108

M

MAC (media access control) addresses	
configured, displaying	90
hardware, displaying	90
major (red) alarms	
action required	154
description	145
PIMs	149
Routing Engine	149
Management Information Bases <i>See</i> MIBs	
management interface address, displaying	85
management interfaces	
active alarms	90
administrative states	90
alarm conditions and configuration options	146
configuration, displaying	90
configuring alarms on	150
monitoring	89, 237
statistics	237
managing	
files	183
reboots	177
snapshots	167
software	159
user authentication and access	3
managing files	183
manuals	
comments on	xx
match conditions, for multicast traffic	241
maximum transmission unit (MTU), displaying	90
media access control <i>See</i> MAC addresses	
memory usage	
for service sets	111
general	85
monitoring <i>See</i> SNMP health monitor	
messages <i>See</i> system log messages	
MIBs (Management Information Bases)	
controlling access (configuration editor)	42
enterprise	32
standard	32
system identification (configuration editor)	39
views (configuration editor)	42
minor (yellow) alarms	
action required	154
alternative boot device	149
description	145
primary compact flash	149
Routing Engine	149
monitor interface command	237
controlling output	237
monitor interface traffic command	237
controlling output	238
monitor list command	237
monitor start command	236
monitor stop command	237
monitor traffic command	239
options	239
performance impact	239
monitor traffic matching command	240
arithmetic, binary, and relational operators	242
logical operators	242
match conditions	241
monitoring	
alarms	152
BGP	93
BGP neighbors, with RPM probes	277
chassis	87
CLI commands and corresponding J-Web	
options	78
DHCP	118
DLSw	97
IDS information	114
IKE security	116
IKE security associations	117
interfaces	89, 237
IPSec tunnels	116

J-Web options and corresponding CLI	
commands	78
Layer 2 circuits	209
Layer 2 VPNs	209
Layer 3 VPNs	209
MPLS traffic engineering	106–110
multicast paths	233
NAT pools	118
network interface traffic	239
network traffic with packet capture	245
OSPF	95
overview	78
<i>See also</i> diagnosis; statistics; status	
ports	89
PPP (CLI)	123
PPPoE	124
preparation	83, 202
RIP	96
routing information	91
routing tables	91
RPM probes	120
service sets	111
services interfaces	111
stateful firewall filters	112
system log messages	129
system logs	236
system process information	87
system properties	84
trace files	236
MPLS (Multiprotocol Label Switching)	
connections, checking	209
LSPs	107
monitoring interfaces	107
monitoring LSP information	107
monitoring LSP statistics	108
monitoring MPLS interfaces	106
monitoring RSVP interfaces	110
monitoring RSVP sessions	109
monitoring traffic engineering	106
mtrace monitor command	235
results	236
mtrace-from-source command	233
options	234
results	235
MTU (maximum transmission unit), displaying	90
multicast	
trace operations, displaying	235
tracing paths	233
multiple routers, using snapshots to replicate configurations	
CLI	172
J-Web	170
Multiprotocol Label Switching <i>See</i> MPLS	

N

name of network interfaces, displaying	89
NAT (Network Address Translation)	
displaying pools	118
monitoring pools	118
neighbors, BGP <i>See</i> BGP neighbors; BGP RPM probes	
network interfaces	
active alarms	90
administrative states	90
alarm conditions and configuration options	146
configuration, displaying	90
configuring alarms on	150
integrated services, alarm conditions and configuration options	146
monitoring	89, 237
monitoring MPLS traffic engineering	107
monitoring traffic	239
monitoring, CoS	99
monitoring, PPPoE	124
monitoring, RSVP	110
packet capture, configuring on	250
packet capture, disabling before changing encapsulation	254
packet capture, supported on	247
services, alarm conditions and configuration options	147
statistics	237
network management	31
automating with operation scripts	68
diagnosis and problem-solving with scripts	68
<i>See also</i> SNMP	
network performance <i>See</i> RPM	
next hop, displaying	92
no-world-readable statement	136
Norton Ghost utility, for compact flash recovery	175
notice icons	xvi
notice logging severity	132
notifications <i>See</i> event policies; system log messages; SNMP traps	
O	
object identifiers (OIDs)	32
OIDs (object identifiers)	32
op command	70
Open Shortest Path First <i>See</i> OSPF	
operation scripts	
disabling	70
enabling	69
executing from the CLI	70
executing within an event policy	71
overview	68
superuser privileges required for	69
/var/db/scripts/op directory	69
operational mode, filtering command output	82
operator login class permissions	7

operators	
arithmetic, binary, and relational operators	242
logical	242
OSPF (Open Shortest Path First)	
monitoring	94
statistics	95
OSPF interfaces	
displaying	95
status	95
OSPF neighbors	
displaying	95
status	95
OSPF routing information	94
outbound time	<i>See</i> RPM probes

P

packet capture	
configuring	251
configuring (J-Web)	218
configuring on an interface	250
disabling	253
disabling before changing encapsulation on	
interfaces	254
displaying configurations	255
displaying firewall filter for	256
enabling	249
encapsulation on interfaces, disabling before	
modifying	254
files	<i>See</i> packet capture files
firewall filters, configuring	251
firewall filters, overview	248
J-Web tool	217
overview	246
overview (J-Web)	217
preparation	249
router interfaces supported	247
verifying captured packets	256
verifying configuration	255
verifying firewall filter for	256
packet capture files	
analyzing	248
libpcap format	257
overview	248
renaming before modifying encapsulation on	
interfaces	254
Packet Capture page	
field summary	219
results	222
packet loss priority, CoS	106
packets	
capturing	245
capturing with J-Web packet capture	217
discarded	91
dropped	91
monitoring jitter	123
monitoring packet loss	122
monitoring round-trip times	122
multicast, tracking	233
packet capture	245
packet capture (J-Web)	217
tracking MPLS	213
tracking with J-Web traceroute	213
tracking with the traceroute command	229
parentheses, in syntax descriptions	xvii
part numbers	89
partitioning a boot medium	172
password	10
retry limits	29
setting login retry limits	29
specifying for authentication	14
<i>See also</i> secret	
password retry limits	
configuring	30
paths, multicast, tracing	233
PCAP	<i>See</i> packet capture
peers, BGP	<i>See</i> BGP neighbors; BGP RPM probes
peers, DLSw	
connection information	98
IP address	97
reachability information	98
performance, monitoring	<i>See</i> RPM
permission bits, for login classes	6
permissions	
denying and allowing commands	7
predefined	7
physdiskwrite utility, for compact flash recovery	175
physical interfaces, CoS	99
PIC	<i>See</i> PIMs
PIMs (Physical Interface Modules)	
failure	149
major (red) alarm	149
PIM number (always 0)	88
ping	
host reachability (CLI)	223
host reachability (J-Web)	204
ICMP probes	270
indications	208
RPM probes	<i>See</i> RPM probes
TCP and UDP probes	274
ping command	223
DHCP server operation	62
DHCP server operation, explanation	63
options	224
Ping end point of LSP	
description	202
using	212
ping host	
results	208
Ping Host page	205
field summary	205

results	207
Ping LDP-signaled LSP	
description	201
using	211
Ping LSP to Layer 3 VPN prefix	
description	202
using	211
ping MPLS (J-Web)	
indications	213
Layer 2 circuits	209
Layer 2 VPNs	209
Layer 3 VPNs	209
LSP state	209
options	201
requirements	203
results	213
ping mpls l2circuit command	229
results	213
ping mpls l2vpn command	227
results	213
ping mpls l3vpn command	227
results	213
ping mpls ldp command	226
results	213
ping mpls lsp-end-point command	226
results	213
Ping MPLS page	210
field summary	210
results	213
ping mpls rsvp command	226
results	213
Ping RSVP-signaled LSP	
description	201
using	210
pipe () command, to filter output	82
Point-to-Point Protocol (PPP), monitoring (CLI)	123
Point-to-Point Protocol over Ethernet <i>See</i> PPPoE	
ports	
alarm conditions and configuration options	146
configuration, displaying	90
configuring alarms on	150
console port, securing	26
DHCP interface restrictions	49
individual port types	146
monitoring	89
PPP (Point-to-Point Protocol), monitoring (CLI)	123
PPPoE (Point-to-Point Protocol over Ethernet)	
interfaces	124
monitoring	124
session status	124
statistics	125
version information	127
primary compact flash <i>See</i> compact flash	
printf statements	68

probe loss	
monitoring	122
threshold, setting	267
probes, monitoring	120, 124
<i>See also</i> RPM probes	
process command, displaying	87
process ID, displaying	87
process information, system, monitoring	87
process owner, displaying	87
process sleep state, displaying	87
process start time, displaying	87
process status, displaying	87
process terminal, displaying	87
properties, system, monitoring	84
protocol version, DLSw	97
protocols	
DHCP <i>See</i> DHCP	
DLSw, monitoring	97
originating, displaying	92
OSPF, monitoring	94
PPP, monitoring	123
RIP, monitoring	96
routing protocols, monitoring	91, 93

Q

Quick Configuration

Add a RADIUS Server page	9
Add a TACACS+ Server page	11
Add a User page	15
adding users	14
authentication method	12
DHCP main page	51
DHCP pool page	52
DHCP static binding page	53
RADIUS server	8
RPM pages	264–265
SNMP page	35
TACACS+ server	10
user management	8
Users page	13
View Events page	138

R

RADIUS

adding a server (Quick Configuration)	8
authentication (configuration editor)	17
order of user authentication (configuration editor)	20
secret (configuration editor)	18
secret (Quick Configuration)	10
specifying for authentication (Quick Configuration)	14
random early detection (RED) drop profiles, CoS	101
reachability, DLSw	98
<i>See also</i> host reachability	

- read or write error, Routing Engine 149
- read-only login class permissions 7
- real-time performance monitoring *See* RPM
- reboot immediately
 - with J-Web 178
 - with the CLI 180
- rebooting
 - with J-Web 177
 - with the CLI 180
- recovering compact flash *See* compact flash recovery
- red alarms *See* major alarms
- red Alarms indicator, in J-Web 152
- RED drop profiles, CoS 101
- registration form, for software upgrades 160–161
- regular expressions for filtering system logs 132
- relational operators, for multicast traffic 242
- release notes, URL xv
- remote accounts
 - accessing with SSH (CLI) 28
 - accessing with Telnet (CLI) 27
 - remote template accounts 24
- remote server, upgrading from 163
- remote template accounts 24
- request system halt command 180
 - options 181
- request system reboot command 180
 - options 180
- request system set-encryption-key algorithm des
 - command 192
- request system set-encryption-key command 192
- request system set-encryption-key des unique 192
- request system set-encryption-key unique 192
- request system snapshot command 171
 - options 172
- request system software add validate unlink reboot
 - command 166
- request system software rollback command 167
- request system storage cleanup command 190
- request system storage cleanup dry-run command 190
- rescue configuration, alarm about 149
- Resource Reservation Protocol *See* RSVP
- retry limits for passwords 29
- reverting to a previous configuration file (J-Web) 167
- rewrite rules, CoS 103
- RIP (Routing Information Protocol)
 - monitoring 96
 - statistics 96
- RIP neighbors
 - displaying 96
 - status 97
- RIP routing information 96
- rolling back a configuration file, to downgrade
 - software (CLI) 167
- root login to the console, disabling 27
- rotating files 185, 190
- round-trip time
 - description 261
 - See also* RPM probes
 - threshold, setting 268
- routing
 - monitoring 91
 - traceroute (J-Web) 213
 - traceroute command 229
 - traceroute monitor command 229
- Routing Engine
 - fan failure 149
 - major (red) alarm 149
 - minor (yellow) alarm 149
 - read or write error 149
 - temperature 88
 - too hot 149
 - too warm 149
- routing policies
 - export, displaying 94
 - import, displaying 94
- routing table
 - displaying 92
 - monitoring 91
- RPM (real-time performance monitoring)
 - basic probes (configuration editor) 270
 - BGP monitoring *See* BGP RPM probes
 - inbound and outbound times 262
 - jitter, viewing 123
 - monitoring probes 120
 - overview 260
 - See also* RPM probes
 - preparation 263
 - probe and test intervals 261
 - probe counts 262
 - Quick Configuration 263
 - round-trip times, description 261
 - round-trip times, viewing 122
 - sample graphs 121
 - statistics 261
 - statistics, verifying 281
 - TCP probes (configuration editor) 274
 - tests 261
 - tests, viewing 121
 - threshold values 262
 - tuning probes 276
 - UDP probes (configuration editor) 274
 - verifying probe servers 282
- RPM pages 264–265
 - field summary 266
- RPM probes
 - basic (configuration editor) 270
 - BGP neighbors *See* BGP RPM probes
 - cumulative jitter 123
 - current tests 121
 - DSCP bits (Quick Configuration) 267

graph results	121	TACACS + (configuration editor)	19
ICMP (configuration editor)	270	TACACS + (Quick Configuration)	12
inbound times	262	<i>See also</i> password	
jitter threshold	268	security	
monitoring	120	access privileges	5, 21
outbound times	262	configuration file encryption	191
probe count, setting (Quick Configuration)	267	<i>See also</i> file encryption	
probe count, tuning	277	console port security	26
probe counts	262	IDS intrusion detection	114
probe intervals	261	IKE, monitoring security associations	117
probe intervals, setting (Quick Configuration)	267	packet capture for intrusion detection	246
probe intervals, tuning	276	password retry limits	29
probe loss count	267	user accounts	4, 23
probe owner	266	user authentication	4
probe type, setting (Quick Configuration)	267	serial cable, disconnection for console logout	27
probe types	260	serial number	
round-trip time threshold	268	chassis components	89
round-trip times, description	261	Services Router	84
round-trip times, viewing	122	serial ports	
SNMP traps (Quick Configuration)	268	alarm condition indicator	154
source address, setting	277	alarm conditions and configuration options	146
TCP (configuration editor)	274	configuring alarms on	150
TCP server port	270	service sets, monitoring	111
test intervals	261	services interfaces, monitoring	111
test intervals, setting (Quick Configuration)	267	services module	
test target	266	alarm condition indicator	154
threshold values, description	262	alarm conditions and configuration options	147
threshold values, setting (Quick Configuration)	267	Services Router	
tuning	276	as a DHCP server	47
UDP (configuration editor)	274	automating operations and troubleshooting	65
UDP server port	270	diagnosis	197
verifying TCP and UDP probe servers	282	halting (CLI)	180
RSVP (Resource Reservation Protocol)		halting (J-Web)	177
interfaces, monitoring	110	monitoring	77
sessions, monitoring	109	network management	31
RTT <i>See</i> RPM probes, round-trip times		packet capture	245
		performance monitoring	259
S		rebooting (CLI)	180
samples		rebooting (J-Web)	177
alarm configuration	154	serial number, displaying	84
basic RPM probes	270	software upgrades	159
DHCP server configuration	60	sessions	
local template account	25	BGP peer, status details	94
RPM test graphs	121	BGP peer, status summary	93
TCP and UDP probes	274	RSVP, monitoring	109
user account	23	Telnet	27
scheduler maps, CoS	104	set no-encrypt-configuration-files command	193
scheduling a reboot		set requests	32
with J-Web	179	set system dump-device command	173
with the CLI	180	options	173
scripts <i>See</i> commit scripts; operation scripts		severity levels	
search, IDS	114	for alarms <i>See</i> alarm severity	
secret	10	for system logs	132
RADIUS (configuration editor)	18	show bgp neighbor command	93
RADIUS (Quick Configuration)	10	show bgp summary command	93

- show chassis alarms command 88, 152, 154
- show chassis environment command 88
- show chassis hardware command 88
- show class-of-service classifier command 100
- show class-of-service code-point-aliases command ... 101
- show class-of-service command 99
- show class-of-service drop-profile command 101
- show class-of-service forwarding-class command 102
- show class-of-service rewrite-rules command 103
- show class-of-service scheduler-map command 104
- show dlsw capabilities command 97
- show dlsw circuits command 97
- show dlsw peers command 97
- show dlsw reachability command 97
- show firewall filter dest-all command 256
- show forwarding-options command 255
- show interfaces detail command 89
- show interfaces interface-name command 89
- show interfaces pp0 command 124
- show interfaces terse command 89
- show log command 131
- show mpls interface command 106
- show mpls lsp command 107
- show mpls statistics command 108
- show ospf interfaces command 94
- show ospf neighbors command 94
- show ospf statistics command 94
- show ppp address-pool command 124
- show ppp interface command 124
- show ppp statistics command 124
- show ppp summary command 124
- show pppoe interfaces command 124
- show pppoe statistics command 124
- show pppoe version command 124
- show rip neighbors command 96
- show rip statistics command 96
- show route detail command 91
- show route terse command 91
- show services ids destination-table command 115
- show services ids pair-table command 115
- show services ids source-table command 115
- show services ipsec-vpn ike command 116
- show services ipsec-vpn ipsec command 116
- show services ipsec-vpn ipsec security-associations
command 116
- show services nat pool command 118
- show services rpm active-servers command 282
- explanation 282
- show services rpm probe-results command 120, 281
- explanation 281
- show services service-sets memory-usage command .. 111
- show services service-sets summary command 111
- show services stateful-firewall conversations
command 114
- show services stateful-firewall flows command 114
- show snmp health-monitor command 44
- show snmp statistics command 44
- show system alarms command 152
- show system processes command 87, 131
- show system services dhcp binding command ... 60, 118
- explanation 61
- show system services dhcp binding detail command .. 60
- explanation 61
- show system services dhcp command 60
- show system services dhcp conflict command 49,
- 60, 118
- explanation 62
- show system services dhcp pool command 60, 118
- show system services dhcp statistics command .. 63, 118
- explanation 64
- show system storage command 84
- show system uptime command 84
- show system users command 84
- Simple Network Management Protocol *See* SNMP
- SMI (Structure of Management Information) 32
- Snapshot page 169
- snapshots
- configuring for failure snapshot storage 173
- to replace primary compact flash, for multiple
 routers (CLI) 172
- to replace primary compact flash, for multiple
 routers (J-Web) 170
- SNMP (Simple Network Management Protocol)
- agents *See* SNMP agents
- communities *See* SNMP communities
- controlling access (configuration editor) 42–43
- get requests 32
- health monitor *See* SNMP health monitor
- managers 31
- MIBs *See* MIBs
- overview 31
- preparation 34
- Quick Configuration 34
- set requests 32
- system identification (configuration editor) 39
- traps *See* SNMP traps
- views (configuration editor) 42
- SNMP agents 31
- configuring (configuration editor) 40
- verifying 44
- SNMP communities
- creating (configuration editor) 40
- description 32
- Quick Configuration 36
- SNMP health monitor
- description 33
- Quick Configuration 34
- verifying 44
- SNMP managers 31
- SNMP page 35

SNMP traps		
automating response to with event policies	71	
creating groups for (configuration editor)	41	
description	33	
performance monitoring <i>See</i> RPM probes		
Quick Configuration	37	
software		
halting immediately (CLI)	181	
halting immediately (J-Web)	179	
upgrades <i>See</i> upgrades		
version, displaying	85	
version, DLSw	97	
SSH		
accessing remote accounts (CLI)	28	
setting login retry limits	29	
ssh command	28	
options	28	
stateful firewall filters		
displaying	114	
flow status	114	
monitoring	112	
static binding, DHCP <i>See</i> DHCP; DHCP leases; DHCP		
server		
statistics		
BGP	93	
DHCP	119	
DHCP server	63	
interfaces	237	
IPSec	116	
LSP	108	
OSPF	95	
performance monitoring	261	
PPPoE	125	
RIP	96	
RPM, description	261	
RPM, monitoring	121	
RPM, verifying	281	
status		
administrative link state	90	
BGP	93–94	
link states	89	
OSPF interfaces	95	
OSPF neighbors	95	
RIP neighbors	97	
stateful firewall filters	114	
storage media		
configuring boot devices	167	
recovering primary compact flash	173	
Structure of Management Information (SMI)	32	
super-user login class permissions	7	
superuser login class permissions	7	
support, technical <i>See</i> technical support		
syntax conventions	xvi	
syslog <i>See</i> system logs		
system identification, displaying	84	
system log messages		
capturing in a file (configuration editor)	134	
destinations	131	
displaying at a terminal (configuration editor)	133, 135	
event viewer	137	
facilities	132	
filtering (Quick Configuration)	138	
monitoring (Quick Configuration)	137	
overview	130	
preparation	134	
regular expressions for filtering	132	
sending messages to a file (configuration editor)	135	
sending messages to a terminal (configuration editor)	135	
severity levels	132	
/var/log directory	134	
viewing (Quick Configuration)	140	
system logs		
archiving	136	
destinations for log files	131	
disabling	136	
displaying size	87	
file cleanup (CLI)	190	
file cleanup (J-Web)	183	
functions	130	
logging facilities	132	
logging severity levels	132	
messages <i>See</i> system log messages		
monitoring	236	
overview	130	
regular expressions for filtering	132	
system management	3	
automating	65	
<i>See also</i> commit scripts; event policies;		
operation scripts		
displaying log and trace file contents	236	
login classes	5, 21	
preparation	8	
Quick Configuration	8	
system logs	129	
template accounts	8, 24	
user accounts	4, 23	
user authentication	4	
system process information, displaying	87	
system storage, displaying	86	
system time, displaying	85	
T		
T1 ports		
alarm conditions and configuration options	146	
configuring alarms on	150	
T3 ports		
alarm condition indicator	154	

- alarm conditions and configuration options 148
 - configuring alarms on 150
 - TACACS +
 - adding a server (Quick Configuration) 10
 - authentication (configuration editor) 18
 - order of user authentication (configuration editor) 20
 - secret (configuration editor) 19
 - secret (Quick Configuration) 12
 - specifying for authentication (Quick Configuration) 14
 - TCP RPM probes
 - description 261
 - server port 270
 - setting 274
 - verifying servers 282
 - technical support
 - contacting JTAC xx
 - hardware information for 88
 - Telnet
 - accessing remote accounts (CLI) 27
 - setting login retry limits 29
 - telnet command 28
 - options 28
 - Telnet session 27
 - temperature
 - chassis, displaying 88
 - Routing Engine, too hot 149
 - Routing Engine, too warm 149
 - template accounts
 - description 8
 - local accounts (configuration editor) 26
 - remote accounts (configuration editor) 25
 - temporary files
 - cleaning up (CLI) 190
 - cleaning up (J-Web) 183
 - displaying size 87
 - downloading (J-Web) 187
 - for packet capture 248
 - terminal session, sending system log messages to 135
 - terminology
 - alarms 143
 - DHCP 47
 - diagnostic 197
 - monitoring 77
 - packet capture 245
 - RPM 259
 - system logs 129
 - user authentication 3
 - tests *See* RPM
 - threshold
 - falling 33
 - rising 33
 - SNMP health monitor 33
 - threshold values, for RPM probes *See* RPM probes
 - time to live *See* TTL
 - time zone, displaying 85
 - trace files
 - monitoring 236
 - multicast, monitoring 235
 - traceroute
 - CLI command 230
 - indications 217
 - J-Web tool 213
 - results 216
 - TTL increments 214
 - traceroute command 230
 - options 230
 - traceroute monitor
 - CLI command 231
 - traceroute monitor command 231
 - options 231
 - results 232
 - Traceroute page 215
 - field summary 215
 - traffic
 - analyzing with packet capture 245
 - multicast, tracking 233
 - tracking with J-Web traceroute 213
 - tracking with the traceroute command 229
 - transmission speed, displaying 90
 - traps *See* SNMP traps
 - troubleshooting
 - automating with event policies 71
 - operation scripts 68
 - See also* diagnosis; operation scripts
 - packet capture for analysis 245
 - See also* diagnosis; packet capture
 - TTL (time to live)
 - default, in multicast path-tracking queries 234
 - in ping requests 208
 - increments, in traceroute packets 214
 - threshold, in multicast trace results 235
 - total, in multicast trace results 235
 - TTY, displaying 85
- ## U
- UDP RPM probes
 - description 261
 - server port 270
 - setting 274
 - verifying servers 282
 - unauthorized login class permissions 7
 - universal serial bus *See* USB
 - upgrades
 - downloading 162
 - installing (CLI) 166
 - installing by uploading 164
 - installing from remote server 163
 - overview 160

requirements.....	160–161
Upload package page.....	165
field summary.....	165
URLs	
release notes.....	xv
software downloads.....	162
USB (universal serial bus)	
configuring.....	172
configuring for failure snapshot storage.....	173
user accounts	
authentication order (configuration editor).....	19
contents.....	4
creating (configuration editor).....	23
for local users.....	25
for remote users.....	24
predefined login classes.....	7
templates for.....	8, 24
<i>See also</i> template accounts	
user logging facility.....	132
username	
description.....	5
displaying.....	85
specifying (Quick Configuration).....	15
users	
access privileges.....	5, 21
accounts <i>See</i> user accounts	
adding (Quick Configuration).....	15
displaying.....	85
login classes.....	5, 21
predefined login classes.....	7
template accounts <i>See</i> template accounts	
usernames.....	5
Users Quick Configuration page.....	13
utilities, for compact flash recovery.....	175

V

/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	
vendor ID, DLSw.....	97
verification	
alarm configurations.....	154

captured packets.....	256
destination path (J-Web).....	213
DHCP binding database.....	60
DHCP server configuration.....	60
DHCP server operation.....	62
DHCP statistics.....	63
firewall filter for packet capture.....	256
host reachability (CLI).....	223
host reachability (J-Web).....	204
LSPs (J-Web).....	209
packet capture.....	255
RPM probe servers.....	282
RPM statistics.....	281
SNMP.....	43
SNMP health monitor.....	44
traceroute command.....	229
traceroute monitor command.....	229
tracing multicast paths.....	233
version	
hardware, displaying.....	89
PPPoE, information about.....	127
software, displaying.....	85
View Events page.....	138
field summary (filtering log messages).....	139
field summary (viewing log messages).....	140
views, SNMP.....	43
VPNs (virtual private networks), no DHCP support on	
interfaces.....	50

W

warning logging severity.....	132
WinZip utility, for compact flash recovery.....	175
world-readable statement.....	136

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	
---------------------------------------	--