J-series™ Services Router

Administration Guide

Release 8.5

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-021979-01, Revision 1

J-series™ Services Router Administration Guide
Release 8.5

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

Revision History
12 October 2007—Revision 1.

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

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 présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés 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

Table of Contents

Chapter 4 Configuring the Router as a DHCP Server 65

Chapter 5 Configuring Autoinstallation 83

Chapter 6 Automating Network Operations and Troubleshooting 91

Part 2 Monitoring a Services Router

Chapter 7 Monitoring the Router and Routing Operations 103

Chapter 14 Configuring RPM Probes 281

Part 5 Index

About This Guide

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

Objectives

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

J-series Services Router operations are controlled by the JUNOS software. You direct the JUNOS software through either a Web browser or a command-line interface (CLI).

NOTE: This guide documents Release 8.5 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.

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.

How to Use This Guide

J-series documentation explains how to install, configure, and manage J-series routers by providing information about JUNOS implementation specifically on J-series routers. (For comprehensive JUNOS information, see the JUNOS software manuals listed in "Related Juniper Networks Documentation" on page xviii.) Table 1 on page xvi shows the location of J-series information, by task type, in Juniper Networks documentation.

Table 1: Location of J-series Information

J-series Tasks	Location of Instruction
Installing hardware and establishing basic connectivity	Getting Started Guide for your router
Configuring interfaces and routing protocols such as RIP, OSPF, BGP, and IS-IS	*J-series Services Router Basic LAN and WAN Access Configuration Guide*
Configuring advanced features such as virtual private networks (VPNs), IP Security (IPSec), multicast, routing policies, firewall filters, and class of service (CoS)	*J-series Services Router Advanced WAN Access Configuration Guide*
Managing users and operations, monitoring performance, upgrading software, and diagnosing common problems	*J-series Services Router Administration Guide*
Using the J-Web interface	*J-Web Interface User Guide*
Using the CLI	*JUNOS CLI User Guide*

Typically, J-series documentation provides both general and specific information—for example, a configuration overview, configuration examples, and verification methods. Because you can configure and manage J-series routers in several ways, you can choose from multiple sets of instructions to perform a task. To make best use of this information:

- *If you are new to the topic*—Read through the initial overview information, keep the related JUNOS guide handy for details about the JUNOS hierarchy, and follow the step-by-step instructions for your preferred interface.
- *If you are already familiar with the feature*—Go directly to the instructions for the interface of your choice, and follow the instructions. You can choose a J-Web method, the JUNOS CLI, or a combination of methods based on the level of complexity or your familiarity with the interface.

For many J-series features, you can use J-Web Quick Configuration pages to configure the router quickly and easily without configuring each statement individually. For more extensive configuration, use the J-Web configuration editor or CLI configuration mode commands.

To monitor, diagnose, and manage a router, use the J-Web interface or CLI operational mode commands.

Document Conventions

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

Table 2: Notice Icons

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

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

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **`show chassis alarms`** `No alarms currently active`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast | multicast (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	■ 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 on page xix.

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	
"Services Router User Interface Overview" "Establishing Basic Connectivity"	■ *JUNOS CLI User Guide* ■ *JUNOS System Basics Configuration Guide*
J-series Services Router Basic LAN and WAN Access Configuration Guide	
"Using Services Router Configuration Tools"	■ *JUNOS CLI User Guide* ■ *JUNOS System Basics Configuration Guide*
"Interfaces Overview" "Configuring DS1, DS3, Ethernet, and Serial Interfaces" "Configuring Channelized T1/E1/ISDN PRI Interfaces" "Configuring Digital Subscriber Line Interfaces "Configuring Point-to-Point Protocol over Ethernet" "Configuring ISDN"	■ *JUNOS Network Interfaces Configuration Guide* ■ *JUNOS Interfaces Command Reference*
"Configuring Link Services Interfaces"	■ *JUNOS Services Interfaces Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
"Configuring VoIP"	■ *JUNOS Network Interfaces Configuration Guide* ■ *JUNOS Interfaces Command Reference*
"Configuring uPIMs as Ethernet Switches"	■ *JUNOS Network Interfaces Configuration Guide* ■ *JUNOS System Basics Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
"Routing Overview" "Configuring Static Routes" "Configuring a RIP Network" "Configuring an OSPF Network" "Configuring the IS-IS Protocol" "Configuring BGP Sessions"	■ *JUNOS Routing Protocols Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference*
J-series Services Router Advanced WAN Access Configuration Guide	

Table 4: J-series Guides and Related JUNOS Software Publications *(continued)*

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
"Multiprotocol Label Switching Overview" "Configuring Signaling Protocols for Traffic Engineering" "Configuring Virtual Private Networks" "Configuring CLNS VPNs"	■ *JUNOS MPLS Applications Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference* ■ *JUNOS VPNs Configuration Guide*
"Configuring IPSec for Secure Packet Exchange"	■ *JUNOS System Basics Configuration Guide* ■ *JUNOS Services Interfaces Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
"Multicast Overview" "Configuring a Multicast Network"	■ *JUNOS Multicast Protocols Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference*
"Configuring Data Link Switching"	■ *JUNOS Services Interfaces Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
"Policy Framework Overview" "Configuring Routing Policies"	■ *JUNOS Policy Framework Configuration Guide* ■ *JUNOS Routing Protocols and Policies Command Reference*
"Configuring NAT" "Configuring Stateful Firewall Filters and NAT" "Configuring Stateless Firewall Filters"	■ *JUNOS Network Interfaces Configuration Guide* ■ *JUNOS Policy Framework Configuration Guide* ■ *JUNOS Services Interfaces Configuration Guide* ■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS* ■ *JUNOS System Basics and Services Command Reference* ■ *JUNOS Routing Protocols and Policies Command Reference*
"Class-of-Service Overview" "Configuring Class of Service"	■ *JUNOS Class of Service Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*
J-series Services Router Administration Guide	
"Managing User Authentication and Access"	■ *JUNOS System Basics Configuration Guide* ■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*
"Configuring SNMP for Network Management"	*JUNOS Network Management Configuration Guide*
"Configuring the Router as a DHCP Server" "Configuring Autoinstallation"	*JUNOS System Basics Configuration Guide*
"Automating Network Operations and Troubleshooting"	*JUNOS Configuration and Diagnostic Automation Guide*

Table 4: J-series Guides and Related JUNOS Software Publications *(continued)*

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
"Monitoring the Router and Routing Operations"	■ *JUNOS System Basics and Services Command Reference* ■ *JUNOS Interfaces Command Reference* ■ *JUNOS Routing Protocols and Policies Command Reference*
"Monitoring Events and Managing System Log Files"	■ *JUNOS System Log Messages Reference* ■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*
"Configuring and Monitoring Alarms"	*JUNOS System Basics Configuration Guide*
"Performing Software Upgrades and Reboots"	*JUNOS Software Installation and Upgrade Guide*
"Using Services Router Diagnostic Tools"	■ *JUNOS System Basics and Services Command Reference* ■ *JUNOS Interfaces Command Reference* ■ *JUNOS Routing Protocols and Policies Command Reference*
"Configuring Packet Capture"	*JUNOS Services Interfaces Configuration Guide*
"Configuring RPM Probes"	*JUNOS System Basics and Services Command Reference*

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

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*.

If the router is operating in a Common Criteria environment, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

User Authentication Terms

Before performing system management tasks, become familiar with the terms defined in Table 5 on page 3.

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

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 14. 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 on page 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 on page 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 on page 5).

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).

Table 6: Permission Bits for Login Classes *(continued)*

Permission Bit	Access
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.
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.

Table 6: Permission Bits for Login Classes *(continued)*

Permission Bit	Access
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 21.

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

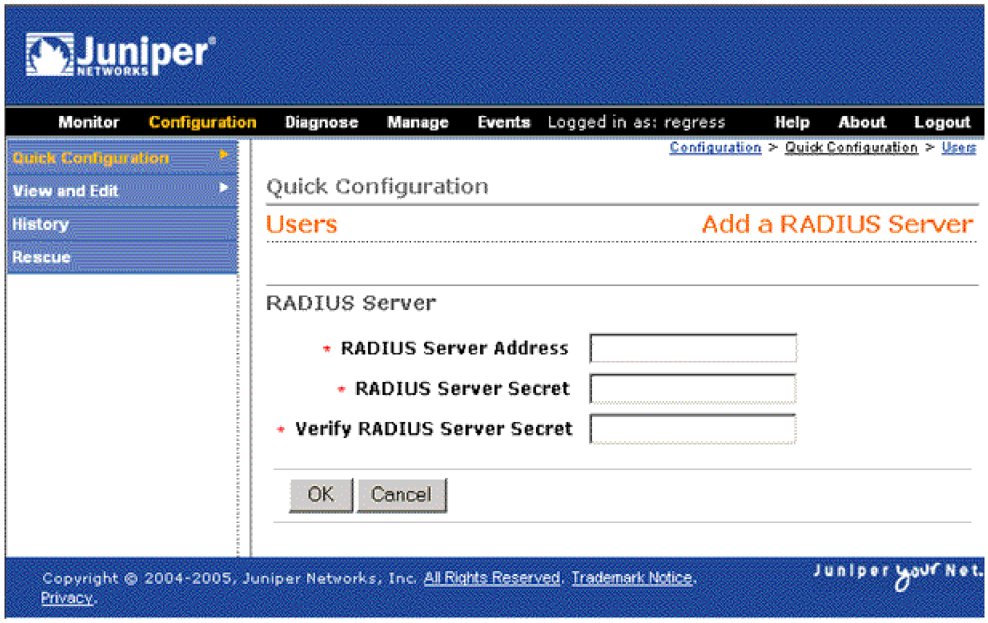
This section contains the following topics:

Adding a RADIUS Server for Authentication

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 on page 9 shows the Users Quick Configuration page for RADIUS servers.

Figure 1: Users Quick Configuration Page for RADIUS Servers



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 on page 9.
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

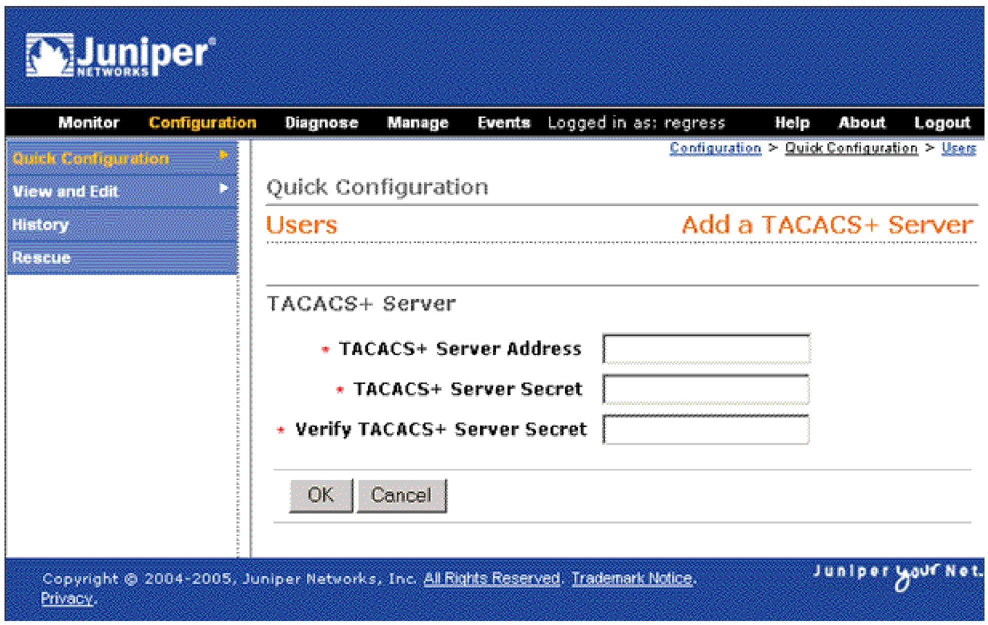
Field	Function	Your Action
RADIUS Server		
RADIUS Server Address (required)	Identifies the IP address of the RADIUS server.	Type the RADIUS server's 32-bit IP address, in dotted decimal notation.
RADIUS Server Secret (required)	The secret (password) of the RADIUS server.	Type the secret (password) of 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 on page 10 shows the Users Quick Configuration page for TACACS+ servers.

Figure 2: Users Quick Configuration Page for TACACS+ Servers



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 on page 10.
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		

Table 9: Users Quick Configuration for TACACS+ Servers Summary *(continued)*

Field	Function	Your Action
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.

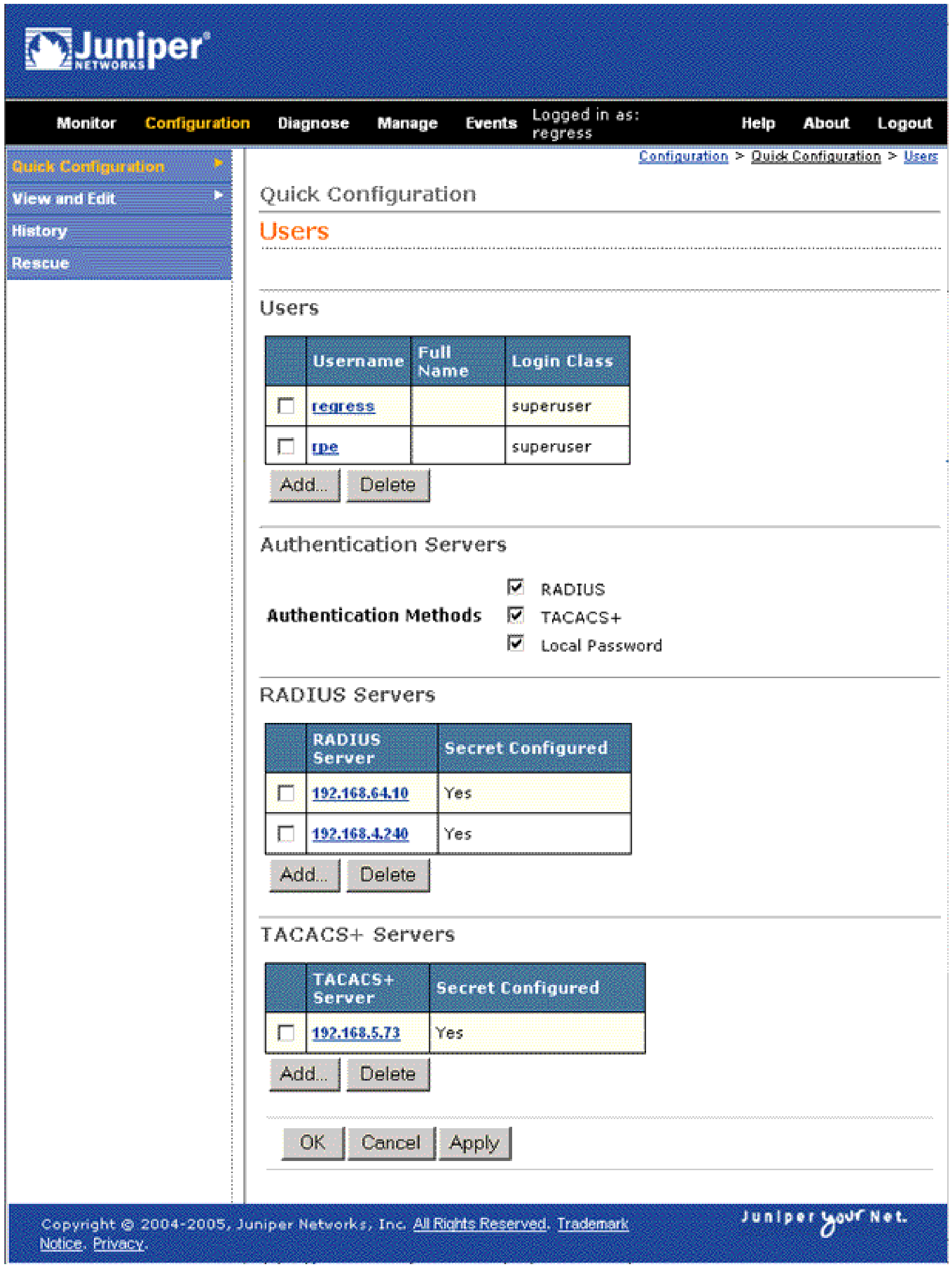
Configuring System Authentication

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 on page 12 shows the Users Quick Configuration page.

Figure 3: Users Quick Configuration Page



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

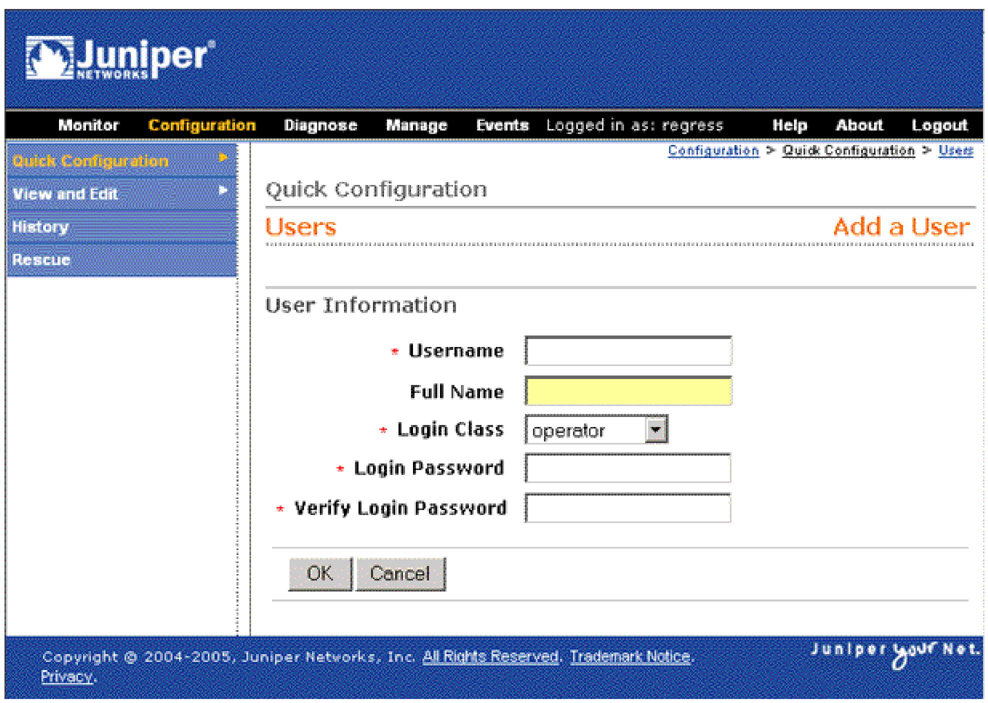
3. Click one of the following buttons on the Users Quick Configuration page:
   - To apply the configuration and stay in the Users Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the Quick Configuration page, click **OK**.
   - To cancel your entries and return 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 on page 13 shows the Quick Configuration page for adding a user.

Figure 4: Add a User Quick Configuration Page



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 on page 14.
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.	From the list, select the user's login class: ■ **operator** ■ **read-only** ■ **super-user/superuser** ■ **unauthorized** This list also includes any user-defined login classes. For more information, see "Login Classes" on page 5.
Login Password (required)	The login password for this user.	Type the login password for this user. The login password must meet the following criteria: ■ The password must be at least 6 characters long. ■ You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters. ■ The password must contain at least one change of case or character class.
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 15
- Setting Up TACACS+ Authentication on page 16
- Configuring Authentication Order on page 17

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 on page 15.
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 17.
   - To configure a remote user template account, see "Creating a Remote Template Account" on page 21.
   - To configure local user template accounts, see "Creating a Local Template Account" on page 22.

Table 11: Setting Up RADIUS Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	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

Table 11: Setting Up RADIUS Authentication *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Add a new RADIUS server	1. In the Radius server box, click **Add new entry**. 2. In the Address box, type the IP address of the RADIUS server: 172.16.98.1	Set the IP address of the RADIUS server: set radius-server address 172.16.98.1
Specify the shared secret (password) of the RADIUS server. The secret is stored as an encrypted value in the configuration database.	In the Secret box, type the shared secret of the RADIUS server: Radiussecret1	Set the shared secret of the RADIUS server: set radius-server 172.16.98.1 secret Radiussecret1
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.	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 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 on page 17.
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 17.

- To configure a remote user template account, see “Creating a Remote Template Account” on page 21.
- To configure local user template accounts, see “Creating a Local Template Account” on page 22.

Table 12: Setting Up TACACS+ Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	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	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 on page 18.
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 15.
   - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 16.
   - To configure a remote user template account, see “Creating a Remote Template Account” on page 21.
   - To configure local user template accounts, see “Creating a Local Template Account” on page 22.

Table 13: Configuring Authentication Order

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	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.	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.	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 18
- Creating User Accounts on page 20

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 20 and “Setting Up Template Accounts” on page 21.

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 on page 19.
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 20.
   - To create shared user accounts, see “Setting Up Template Accounts” on page 21.

Table 14: Defining Login Classes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Login** level in the configuration hierarchy.	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.	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**.	Set the name of the login class and the ability to use the request system reboot command: set class operator-and-boot allow-commands “request system reboot”

Table 14: Defining Login Classes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Give the operator-and-boot login class operator privileges.	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**.	Set the permission bits for the operator-and-boot login class: set class operator-and-boot permissions [clear network reset trace view]

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 15 and “Setting Up TACACS+ Authentication” on page 16.)

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 on page 21.
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.	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 cmartin who belongs to the superuser login class.	1. Next to User, click **Add new entry**. 2. In the User name box, type cmartin. 3. In the Class box, type superuser. 4. Click **OK**.	Set the username and the login class for the user: set user cmartin class superuser
Define the encrypted password for cmartin.	1. Next to Authentication, click **Configure**. 2. In the Encrypted password box, type $1$14c5.$sBopasdFFdssdfFFdsdfs0 3. Click **OK**.	Set the encrypted password for cmartin. set user cmartin authentication encrypted-password $1$14c5.$sBopasdFFdssdfFFdsdfs0

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

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 on page 22.
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 15.
   - To configure a TACACS+ server, see "Setting Up TACACS+ Authentication" on page 16.
   - To specify a system authentication order, see "Configuring Authentication Order" on page 17.

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.	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.	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 on page 23.
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 15.
   - To configure a TACACS+ server, see "Setting Up TACACS+ Authentication" on page 16.
   - To configure a system authentication order, see "Configuring Authentication Order" on page 17.

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.	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.	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

Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.

NOTE: You need console access to recover the root password.

To recover the root password:

1. Power off the router by pressing the power button on the front panel.
2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45 to DB-9 serial port adapter supplied with the router (see Figure 5 on page 24 and Figure 6 on page 25).
4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see Figure 5 on page 24 and Figure 6 on page 25).
5. Connect the other end of the Ethernet rollover cable to the console port on the router (see Figure 5 on page 24 and Figure 6 on page 25).

Figure 5: Connecting to the Console Port on the J2300 Services Router

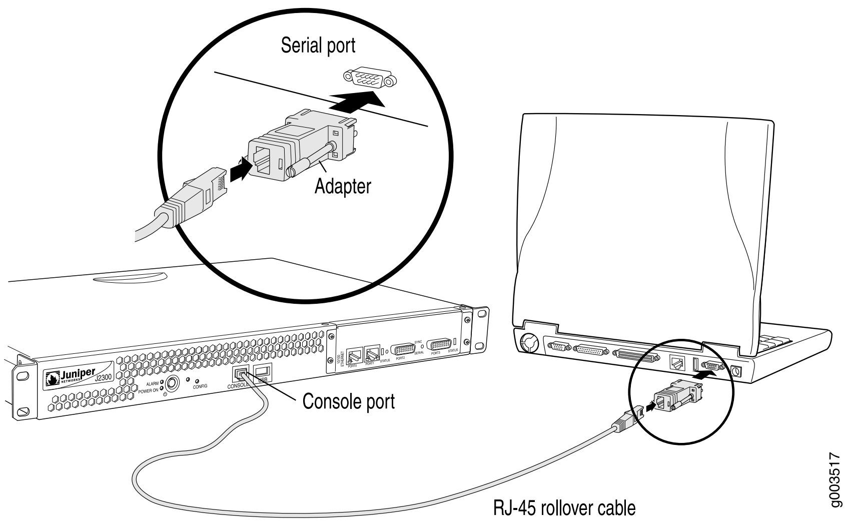
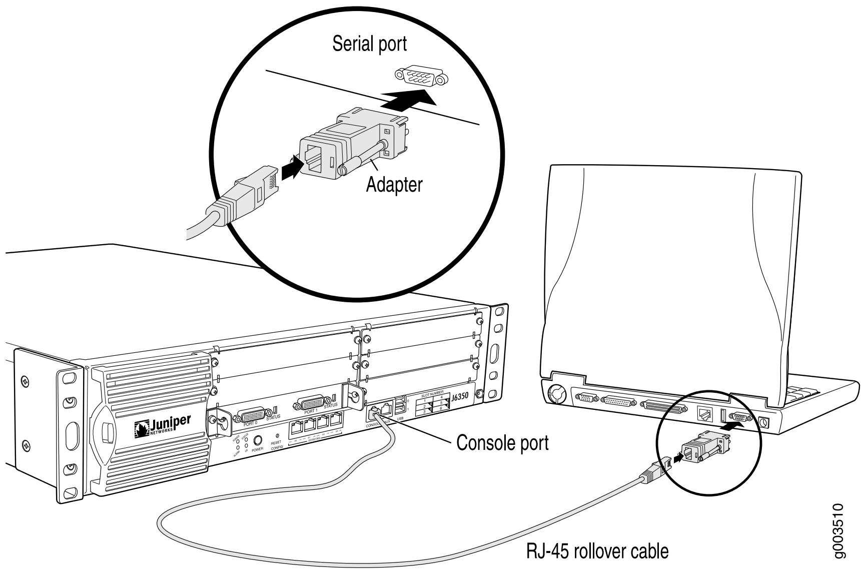


Figure 6: Connecting to the Console Port on the J4350 or J6350 Services Router



6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
9. Power on the router by pressing the power button on the front panel. Verify that the POWER LED on the front panel turns green.

   The terminal emulation screen on your management device displays the router's boot sequence.
10. When the following prompt appears, press the Spacebar to access the router's bootstrap loader command prompt:

```
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel] in 9 seconds...
```

11. At the following prompt, enter **boot -s** to start up the system in single-user mode.

```
ok boot -s
```

12. At the following prompt, enter recovery to start the root password recovery procedure.

```
Enter full pathname of shell or 'recovery' for root password recovery or
RETURN for /bin/sh: recovery
```

13. Enter configuration mode in the CLI.
14. Set the root password. For example:

```
user@host# set system root-authentication plain-text-password
```

    For more information about configuring the root password, see the *JUNOS System Basics Configuration Guide*.

15. At the following prompt, enter the new root password. For example:

```
New password: juniper1

Retype new password:
```

16. At the second prompt, reenter the new root password.
17. If you are finished configuring the network, commit the configuration.

```
root@host# commit

commit complete
```

18. Exit configuration mode in the CLI.
19. Exit operational mode in the CLI.
20. At the prompt, enter y to reboot the router.

```
Reboot the system? [y/n] y
```

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).

In a Common Criteria environment, you *must* disable the console port. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

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 on page 27.
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.	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.	1. Select one of the following check boxes: ■ **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: ■ 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-]. To exit from the Telnet session and return to the CLI command prompt, enter **quit**.

Table 19 on page 28 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 *source-interface*	Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.
no-resolve	Suppress the display of symbolic names.
port *port*	Specify the port number or service name on the host.
routing-instance *routing-instance-name*	Use the specified routing instance for the Telnet session.
source *address*	Use the specified source address for the Telnet session.

Using the ssh Command

You can use the CLI **ssh** command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```

Table 20 on page 28 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.

Table 20: CLI ssh Command Options *(continued)*

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

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 on page 30.
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.	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. ■ 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.	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**.	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

Setting Up USB Modems for Remote Management

J-series Services Routers support the use of USB modems for remote management. You can use Telnet or SSH to connect to the router from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the Services Router, and a second modem is connected to a remote management device such as a PC or laptop computer.

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

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

This chapter contains the following topics:

USB Modem Terms

Before configuring USB modems and their supporting dialer interfaces, become familiar with the terms defined in Table 22 on page 32.

Table 22: USB Modem Terminology

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

USB Modem Overview

A USB modem connects to a Services Router through modem interfaces that you configure. The router applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the router and the modem at the user end of the network.

- USB Modem Interfaces on page 32
- How a Services Router Initializes USB Modems on page 33
- USB Modem Connection and Configuration Overview on page 34

USB Modem Interfaces

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

- The USB modem physical interface uses the naming convention umd0. The Services Router creates this interface when a USB modem is connected to the USB port.
- The dialer interface, dl*n*, is a logical interface for configuring dialing properties for USB modem connections.

See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- The dialer interface cannot be configured as a constituent link in a multilink bundle.
- If you are using the same dialer interface for ISDN connections and USB modem connections, the dialer interface cannot be configured simultaneously in the following modes:
  - As a backup interface and a dialer filter
  - As a backup interface and dialer watch interface
  - As a dialer watch interface and a dialer filter
  - As a backup interface for more than one primary interface

How a Services Router Initializes USB Modems

When you connect the USB modem to the USB port on the Services Router, the router applies the modem AT commands configured in the init-command-string command to the initialization commands on the modem. For more information about configuring modem commands for the init-command-string command, see "Modifying USB Modem Initialization Commands" on page 43.

If you do not configure modem AT commands for the init-command-string command, the router applies the following default sequence of initialization commands to the modem: AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0. Table 23 on page 33 describes the commands. For more information about these commands, see the documentation for your modem.

Table 23: J-series Default Modem Initialization Commands

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

Table 23: J-series Default Modem Initialization Commands *(continued)*

Modem Command	Description
%C0	Disables data compression.

When the Services Router applies the modem AT commands in the init-command-string command or the default sequence of initialization commands to the modem, it compares them to the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the router overrides existing modem values that do not match. For example, if the initialization commands on the modem include S0=0 and the router's init-command-string command includes S0=2, the Services Router applies S0=2.
- If the initialization commands on the modem do not include a command in the router's init-command-string command, the router adds it. For example, if the init-command-string command includes the command L2, but the modem commands do not include it, the router adds L2 to the initialization commands configured on the modem.

USB Modem Connection and Configuration Overview

To use USB modems to remotely manage a Services Router, you perform the tasks listed in Table 24 on page 34. For instructions, see the cross-references in the table.

Table 24: USB Modem Connection and Configuration Overview

Task	Instructions
Perform prerequisite tasks.	"Before You Begin" on page 35
On the Services Router	
1. Connect a modem to the router.	"Connecting the USB Modem to the Services Router's USB Port" on page 35
2. Configure the modem interfaces on the router.	"Configuring USB Modem Interfaces with a Configuration Editor" on page 35
3. Verify the modem configuration on the router.	"Verifying the USB Modem Configuration" on page 44
4. Perform administrative tasks as necessary.	■ Modifying USB Modem Initialization Commands on page 43 ■ Resetting USB Modems on page 44
At the User End	
1. Configure the modem at your remote location.	"Configuring a Dial-Up Modem Connection at the User End" on page 41
2. Dial in to the router.	"Connecting to the Services Router from the User End" on page 42

Before You Begin

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

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

Connecting the USB Modem to the Services Router's USB Port

NOTE: J4350 and J6350 Services Routers have two USB ports. However, you can connect only one USB modem to the USB ports on these routers. If you connect USB modems to both ports, the router detects only the first modem connected.

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

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

Configuring USB Modem Interfaces with a Configuration Editor

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

- Configuring a USB Modem Interface (Required) on page 35
- Configuring a Dialer Interface (Required) on page 37
- Configuring Dial-In (Required) on page 38
- Configuring CHAP on Dialer Interfaces (Optional) on page 39

Configuring a USB Modem Interface (Required)

To configure a USB modem interface for the Services Router:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 25 on page 36.
3. Go on to “Configuring a Dialer Interface (Required)” on page 37.

Table 25: Configuring a USB Modem Interface

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Interfaces** level in the configuration hierarchy.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to Interfaces, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit interfaces umd0
Create the new interface umd0.	1. Next to Interface, click **Add new entry**. 2. In the Interface name box, type the name of the new interface, umd0. 3. Click **OK**.	
Configure dialer options. ■ Name the dialer pool configured on the dialer interface you want to use for USB modem connectivity—for example, usb-modem-dialer-pool. For more information, see “Configuring a Dialer Interface (Required)” on page 37. ■ Set the dialer pool priority—for example, 25. Dialer pool priority has a range from 1 to 255, with 1 designating lowest-priority interfaces and 255 designating the highest-priority interfaces.	1. In the Encapsulation column, next to the new interface, click **Edit**. 2. Next to Dialer options, select **Yes**, and then click **Configure**. 3. Next to Pool, click **Add new entry**. 4. In the Pool identifier box, type usb-modem-dialer-pool. 5. In the Priority box, type 25. 6. Click **OK** until you return to the Interface page.	Enter set dialer-options pool usb-modem-dialer-pool priority 25
The S0=0 command in the default modem initialization sequence AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0, disables the modem from automatically answering calls. Configure the modem to automatically answer calls after a specified number of rings. For more information about modem initialization commands, see “How a Services Router Initializes USB Modems” on page 33 and “Modifying USB Modem Initialization Commands” on page 43.	1. Next to Modem options, click **Configure**. 2. In the Init command string box, type ATS0=2 to configure the modem to automatically answer after two rings. 3. Click **OK**.	Enter set modem-options init-command-string "ATS0=2 \n"

Configuring a Dialer Interface (Required)

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

To configure a logical dialer interface for the Services Router:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 26 on page 37.
3. Go on to "Configuring Dial-In (Required)" on page 38.

Table 26: Adding a Dialer Interface to a Services Router

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Interfaces** level in the configuration hierarchy.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to Interfaces, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit interfaces
Create the new interface—for example, dl0. Adding a description can differentiate between different dialer interfaces—for example, USB-modem-remote-management.	1. Next to Interface, click **Add new entry**. 2. In the Interface name box, type dl0. 3. In the Description box, type USB-modem-remote-management. 4. Click **OK**.	Create and name the interface: 1. edit dl0 2. set description USB-modem-remote-management
Configure Point-to-Point Protocol (PPP) encapsulation. **NOTE:** You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.	1. In the Encapsulation column, next to the new interface, click **Edit**. 2. From the Encapsulation list, select **ppp**.	Enter set encapsulation ppp
Create the logical unit 0. **NOTE:** The logical unit number must be 0.	1. Next to Unit, click **Add new entry**. 2. In the Interface unit number box, type 0. 3. Next to Dialer options, select **Yes**, and then click **Configure**.	Enter set unit 0

Table 26: Adding a Dialer Interface to a Services Router *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the name of the dialer pool to use for USB modem connectivity—for example, usb-modem-dialer-pool.	1. In the Pool box, type usb-modem-dialer-pool. 2. Click **OK**.	1. Enter edit unit 0 2. Enter set dialer-options pool usb-modem-dialer-pool
Configure source and destination IP addresses for the dialer interface—for example, 172.20.10.2 and 172.20.10.1. **NOTE:** If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The router might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.	1. Select **Inet** under Family, and click **Configure**. 2. Next to Address, click **Add new entry**. 3. In the Source box, type 172.20.10.2. 4. In the Destination box, type 172.20.10.1. 5. Click **OK**.	Enter set family inet address 172.20.10.2 destination 172.20.10.1

Configuring Dial-In (Required)

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the Services Router matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the Services Router performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

To configure a dialer interface for dial-in:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 27 on page 39.

3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the USB Modem Configuration” on page 44.

Table 27: Configuring the Dialer Interface for Dial-In

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Interfaces** level in the configuration hierarchy, and select a dialer interface—for example, dl0.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to Interfaces, click **Edit**. 3. Next to dl0, click **Edit**.	From the [edit] hierarchy level, enter edit interfaces dl0
On logical interface 0 configure the incoming map options for the dialer interface. ■ accept-all—Dialer interface accepts all incoming calls. You can configure the accept-all option for only one of the dialer interfaces associated with a USB modem physical interface. The router uses the dialer interface with the accept-all option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces. ■ caller—Dialer interface accepts calls from a specific caller ID—for example, 4085550115. You can configure a maximum of 15 caller IDs per dialer interface. The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.	1. In the Unit section, for logical unit number 0, click **Dialer options** under Nested Configuration. 2. Next to Incoming map, click **Configure**. 3. From the Caller type menu, select **Caller**. 4. Next to Caller, click **Add new entry**. 5. In the Caller id box, type 4085550115. 6. Click **OK**. 7. Repeat Steps 4 through 6 for each caller ID to be accepted on the dialer interface.	1. Enter edit unit 0 2. Enter edit dialer-options 3. Enter set incoming-map caller 4085550115 4. Repeat Step 3 for each caller ID to be accepted on the dialer interface.

Configuring CHAP on Dialer Interfaces (Optional)

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

For more information about CHAP, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide* and the *JUNOS Network Interfaces Configuration Guide*.

To configure CHAP on the dialer interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 28 on page 40.
3. If you are finished configuring the router, commit the configuration.
4. To verify the CHAP configuration, see "Verifying the USB Modem Configuration" on page 44.

Table 28: Configuring CHAP on Dialer Interfaces

Task	J-Web Configuration Editor	CLI Configuration Editor
Define a CHAP access profile—for example, usb-modem-access-profile with a client (username) named usb-modem-user and the secret (password) my-secret.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to Access, click **Configure** or **Edit**. 3. Next to Profile, click **Add new entry**. 4. In the Profile name box, type usb-modem-access-profile. 5. Next to Client, click **Add new entry**. 6. In the Name box, type usb-modem-user. 7. In the Chap secret box, type my-secret. 8. Click **OK**. 9. Repeat Steps 5 through 8 for each client to be included in the CHAP profile. 10. Click **OK** until you return to the Configuration page.	1. From the [edit] hierarchy level, enter edit access 2. Enter set profile usb-modem-access-profile client usb-modem-user chap-secret my-secret 3. Repeat Step 2 for each client to be included in the CHAP profile.
Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, dl0 unit 0.	1. On the Configuration page next to Interfaces, click **Edit**. 2. In the Interface name column, click **dl0**. 3. Under Unit, in the Interface unit number column, click **0**.	From the [edit] hierarchy level, enter edit interfaces dl0 unit 0
Configure CHAP on the dialer interface and specify a unique profile name containing a client list and access parameters—for example, usb-modem-access-profile. **NOTE:** Do not configure the passive option from the [edit interfaces dl0 unit 0 ppp-options chap] hierarchy level.	1. Next to Ppp options, click **Configure**. 2. Next to Chap, click **Configure**. 3. In the Access profile box, type usb-modem-access-profile. 4. Click **OK**.	Enter set ppp-options chap access-profile usb-modem-access-profile

Connecting to the Services Router from the User End

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

This section contains the following topics:

- Configuring a Dial-Up Modem Connection at the User End on page 41
- Connecting to the Services Router from the User End on page 42

Configuring a Dial-Up Modem Connection at the User End

To remotely connect to the USB modem connected to the USB port on the Services Router, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection at the user end:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. Connect the modem to your telephone network.
3. On the PC or laptop computer, select **Start > Settings > Control Panel > Network Connections**.

   The Network Connections page is displayed.
4. Click **Create a new connection**.

   The New Connection Wizard is displayed.
5. Click **Next**.

   The New Connection Wizard: Network Connection Type page is displayed.
6. Select **Connect to the network at my workplace**, and then click **Next**.

   The New Connection Wizard: Network Connection page is displayed.
7. Select **Dial-up connection**, and then click **Next**.

   The New Connection Wizard: Connection Name page is displayed.
8. In the Company Name box, type the dial-up connection name—for example, USB-modem-connect—and then click **Next**.

   The New Connection Wizard: Phone Number to Dial page is displayed.
9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the router end.

10. Click **Next** twice, and then click **Finish**.

    The Connect USB-modem-connect page is displayed.

11. If CHAP is configured on the dialer interface used for the USB modem interface at the router end, type the username and password configured in the CHAP configuration in the User name and Password boxes. For information about configuring CHAP on dialer interfaces, see "Configuring CHAP on Dialer Interfaces (Optional)" on page 39.

12. Click **Properties**.

    The USB-modem-connect Properties page is displayed.

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

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

14. Click **Advanced**.

    The Advanced TCP/IP Settings page appears.

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

Connecting to the Services Router from the User End

To remotely connect to the Services Router through a USB modem connected to the USB port on the router:

1. On the PC or laptop computer at your remote location, select **Start > Settings > Control Panel > Network Connections**.

   The Network Connections page is displayed.

2. Double-click the **USB-modem-connect** dial-up connection configured in "Configuring a Dial-Up Modem Connection at the User End" on page 41.

   The Connect USB-modem-connect page is displayed.

3. Click **Dial** to connect to the Services Router.

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

Administering USB Modems

This section contains the following topics:

Modifying USB Modem Initialization Commands

NOTE: These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands.

You can use the J-Web or CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.

NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.

In this example, you override the value of the S0=0 command in the initialization sequence configured on the modem and add the L2 command.

To modify the initialization commands on a USB modem:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 29 on page 43.
3. If you are finished configuring the router, commit the configuration.
4. To verify that the initialization commands are configured correctly, see "Verifying the USB Modem Configuration" on page 44.

Table 29: Modifying USB Modem Initialization Commands

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Interfaces** level in the configuration hierarchy.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to Interfaces, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit interfaces umd0

Table 29: Modifying USB Modem Initialization Commands *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the modem AT commands to initialize the USB modem. For example: ■ The command S0=2 configures the modem to automatically answer calls on the second ring. ■ The command L2 configures medium speaker volume on the modem. You can insert spaces between commands. When you configure modem commands in the CLI configuration editor, you must follow these conventions: ■ Use the newline character \n to indicate the end of a command sequence. ■ Enclose the command string in double quotation marks.	1. Next to Modem options, click **Configure**. 2. In the Init command string box, type AT S0=2 L2. 3. Click **OK**.	From the [edit interfaces umd0] hierarchy, enter set modem-options init-command-string "AT S0=2 L2 \n"

Resetting USB Modems

If the USB modem does not respond, you can reset the modem.

CAUTION: If you reset the modem when a call is in progress, the call is terminated.

To reset the USB modem:

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

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

Verifying the USB Modem Configuration

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

- Verifying a USB Modem Interface on page 45
- Verifying Dialer Interface Configuration on page 46

Verifying a USB Modem Interface

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

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

```
user@host> show interfaces umd0 extensive
Physical interface: umd0, Enabled, Physical link is Up
  Interface index: 64, SNMP ifIndex: 33, Generation: 1
  Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
Clocking: Unspecified, Speed: MODEM
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : None
  Hold-times     : Up 0 ms, Down 0 ms
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :               21672
   Output bytes  :               22558
   Input  packets:                1782
   Output packets:                1832
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
 0,
Resource errors: 0
  Output errors:
    Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
 0
  MODEM status:
    Modem type                  : LT V.92 1.0 MT5634ZBA-USB-V92 Data/Fax Modem

(Dual Config) Version 2.27m
    Initialization command string : ATS0=2
    Initialization status         : Ok
    Call status                   : Connected to 4085551515
    Call duration                 : 13429 seconds
    Call direction                : Dialin
    Baud rate                     : 33600 bps
    Most recent error code        : NO CARRIER

  Logical interface umd0.0 (Index 2) (SNMP ifIndex 34) (Generation 1)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PPP-Subordinate
```

What It Means The output shows a summary of interface information and displays the modem status.

Verify the following information:

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

  - In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces** > *interface-name* page.

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

  For more information, see "Modifying USB Modem Initialization Commands" on page 43.
- The modem initialization status is Ok. If the initialization status is shown as Error or Not Initialized, do the following:
  1. Verify that the modem initialization commands are valid. If the modem initialization sequence includes invalid commands, correct them, as described in "Modifying USB Modem Initialization Commands" on page 43.
  2. If the modem initialization commands are valid, reset the modem. For more information, see "Resetting USB Modems" on page 44.

Determine the following information:

- The call status
- The duration of the call

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

Verifying Dialer Interface Configuration

Purpose Verify that the dialer interface is correctly configured.

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

```
user@host> show interfaces dl0 extensive
Physical interface: dl0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed:
Unspecified
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
```

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

  Logical interface dl0.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
    Description: USB-modem-remote-management
    Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
    Dialer:
      State: Active, Dial pool: usb-modem-dialer-pool
      Dial strings: 220
      Subordinate interfaces: umd0 (Index 64)
      Activation delay: 0, Deactivation delay: 0
      Initial route check delay: 120
      Redial delay: 3
      Callback wait period: 5
      Load threshold: 0, Load interval: 60
    Bandwidth: 115200
    Traffic statistics:
     Input  bytes  :              24839
     Output bytes  :              17792
     Input  packets:                489
     Output packets:                340
    Local statistics:
     Input  bytes  :              10980
     Output bytes  :              17792
     Input  packets:                172
     Output packets:                340
    Transit statistics:
     Input  bytes  :              13859                   0 bps
     Output bytes  :                  0                   0 bps
     Input  packets:                317                   0 pps
     Output packets:                  0                   0 pps
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
  CHAP state: Success
    Protocol inet, MTU: 1500, Generation: 136, Route table: 0
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 172.20.10.1, Local: 172.20.10.2, Broadcast: Unspecified,
Generation: 134
```

What It Means The output shows a summary of dialer interface information. Verify the following information:

- The physical interface is Enabled. If the interface is shown as Disabled, do either of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces *interface-name*] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces >** *interface-name* page.
- The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- The Last Flapped time is an expected value. The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates possible link-layer errors.
- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics *interface-name* command.
- The dialer state is Active when a USB modem call is in progress.
- The LCP state is Opened when a USB modem call is in progress. An LCP state of Closed or Not Configured indicates a problem with the dialer configuration that needs to be debugged with the monitor traffic interface *interface-name* command. For information about the monitor traffic command, see “Using the monitor traffic Command” on page 260.

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

Chapter 3

Configuring SNMP for Network Management

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

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

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

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

SNMP Architecture

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

Because SNMP is a client/server protocol, SNMP nodes can be classified as either clients (SNMP managers) or servers (SNMP agents). SNMP managers, also called network management systems (NMSs), occupy central points in the network and actively query and collect messages from SNMP agents in the network. SNMP agents are individual processes running on network nodes that gather information for a particular node and transfer the information to SNMP managers as queries are processed. The agent also controls access to the agent's Management Information Base (MIB), the collection of objects that can be viewed or changed by the SNMP manager. Because SNMP agents are individual SNMP processes running on a host, multiple agents can be active on a single network node at any given time.

Communication between the agent and the manager occurs in one of the following forms:

- Get, GetBulk, and GetNext requests—The manager requests information from the agent, and the agent returns the information in a Get response message.
- Set requests—The manager changes the value of a MIB object controlled by the agent, and the agent indicates status in a Set response message.
- Traps notification—The agent sends traps to notify the manager of significant events that occur on the network device.

Management Information Base

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

MIBs are either standard or enterprise-specific. Standard MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Depending on the vendor, many standard MIBs are delivered with the NMS software. You can also download the standard MIBs from the IETF Web site, http://www.ietf.org, and compile them into your NMS, if necessary.

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

Enterprise-specific MIBs are developed and supported by a specific equipment manufacturer. If your network contains devices that have enterprise-specific MIBs, you must obtain them from the manufacturer and compile them into your network management software.

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

SNMP Communities

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

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

SNMP Traps

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

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

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

Spoofing SNMP Traps

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

SNMP Health Monitor

The SNMP health monitor feature uses existing SNMP remote monitoring (RMON) alarms and traps to monitor a select set of Services Router characteristics (object instances) like the CPU usage, memory usage, and file system usage. The health monitor feature also monitors the CPU usage of the 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

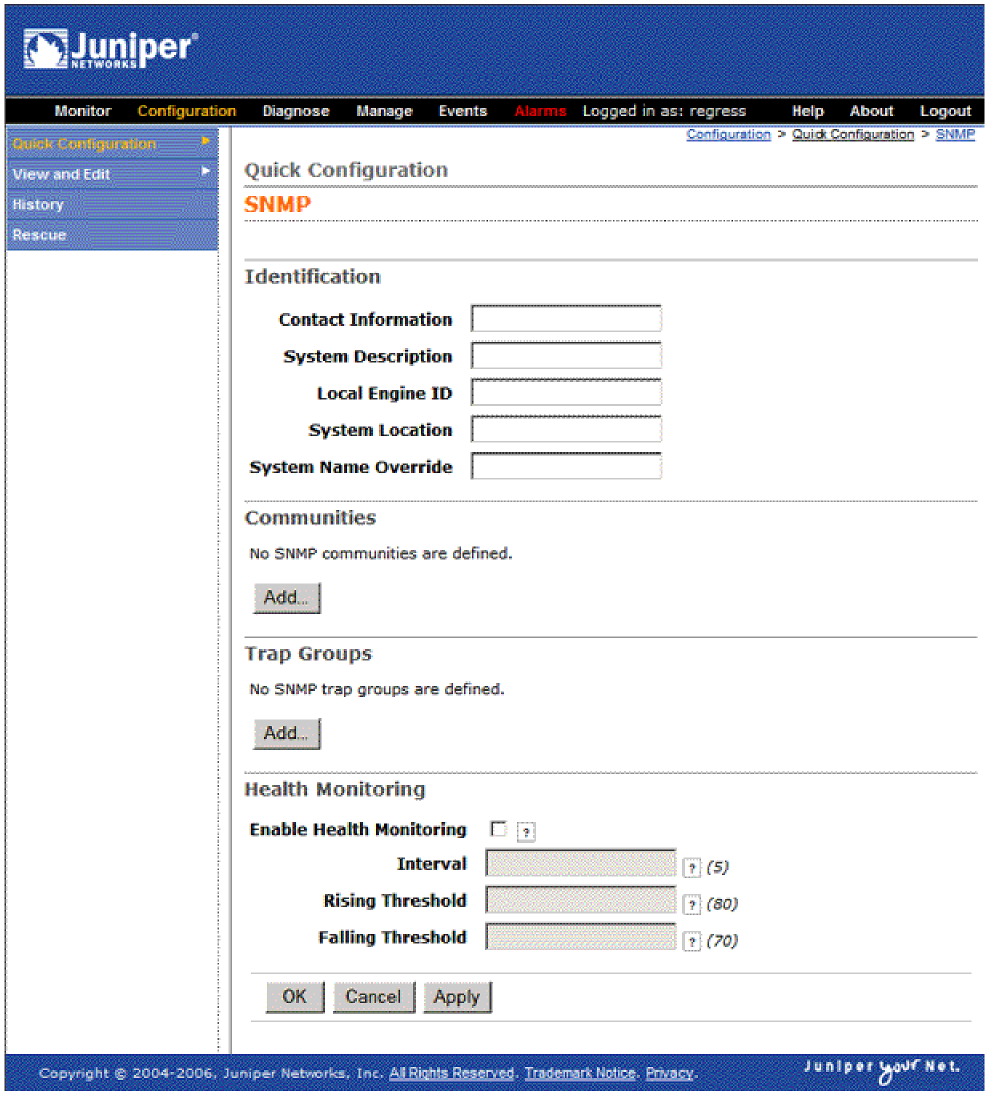
Before you begin configuring SNMP, complete the following tasks:

- 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 7 on page 53 shows the Quick Configuration page for SNMP.

Figure 7: Quick Configuration Page for SNMP



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 30 on page 54.
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 61.

Table 30: 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 (*J4300 with 4 PIMs*, for example).
Local Engine ID	Provides an administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.	Type the MAC address of Ethernet management port 0.
System Location	Free-form text string that specifies the location of the system.	Type any location information for the system (lab name or rack name, for example).
System Name Override	Free-form text string that overrides the system hostname.	Type the name of the system.
Communities		Click **Add**.
Community Name	Specifies the name of the SNMP community.	Type the name of the community being added.
Authorization	Specifies the type of authorization (either read-only or read-write) for the SNMP community being configured.	Select the desired authorization (either read-only or read-write) from the list.
Traps		Click **Add**.
Trap Group Name	Specifies the name of the SNMP trap group being configured.	Type the name of the SNMP trap group being configured.

Table 30: SNMP Quick Configuration Summary *(continued)*

Field	Function	Your Action
Categories	Specifies which trap categories are added to the trap group being configured.	■ 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.	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 30: SNMP Quick Configuration Summary *(continued)*

Field	Function	Your Action
Enable Health Monitoring	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: ■ 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	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. **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.
Interval	Determines the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds. For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.	Enter an interval time, in seconds, between 1 and 2147483647. The default value is 300 seconds (5 minutes).
Rising Threshold	Value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is *increasing*. 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.	Enter a value between 0 and 100. The default value is 90.
Falling Threshold	Value at which you want SNMP to generate an event (trap and system log message) when the value of a sampled indicator is *decreasing*. 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.	Enter a value between 0 and 100. The default value is 80. **NOTE:** The falling threshold value must be less than the rising threshold value.

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 57
- Configuring SNMP Agents and Communities (Required) on page 58
- Managing SNMP Trap Groups (Required) on page 59
- Controlling Access to MIBs (Optional) on page 60

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 31 on page 57 identifies types of basic system identification and the MIB object into which each type is stored.

Table 31: 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 32 on page 57.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 61.

Table 32: Configuring Basic System Identification

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	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

Table 32: Configuring Basic System Identification *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the system contact information (such as a name and phone number).	In the Contact box, type the contact information as a free-form text string.	Set the contact information: set contact "*contact-information*"
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 "*location-information*"
Configure the system description (*J4300 with 4 PIMs*, for example).	In the Description box, type the description information as a free-form text string.	Set the description information: set description "*description-information*"
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 *name*
Configure the local engine ID to use the MAC address of Ethernet management port 0 as the engine ID suffix.	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 33 on page 59.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 61.

Table 33: Configuring SNMP Agents and Communities

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	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
Create and name a community.	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: set community *community-name*
Grant read-write access to the community.	In the Authorization box, select **read-write** from the list.	Set the authorization to read-write: set community *community-name* authorization read-write
Allow community access to a client at a particular IP address—for example, at IP address 10.10.10.10.	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: set community *community-name* clients 10.10.10.10
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.	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**.	1. Configure client access for the IP address 10.10.10.0/24: set community *community-name* clients 10.10.10.0/24 2. Configure client access to restrict the IP addresses 10.10.10.10/29: set community *community-name* clients 10.10.10.10/29 restrict

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 34 on page 60.

3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 61.

Table 34: Configuring SNMP Trap Groups

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	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
Create a trap group.	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: set trap-group *trap-group-name*
Configure the trap group to send all trap notifications to a target IP address—for example, to the IP address 192.174.6.6.	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: set trap-group *trap-group-name* targets 192.174.6.6
Configure the trap group to generate SNMP notifications on authentication failures, environment alarms, and changes in link state for any of the interfaces.	1. Click **Categories**. 2. Select the **Authentication**, **Chassis**, and **Link** check boxes. 3. Click **OK**.	Configure the trap group categories: set trap-group *trap-group-name* categories authentication chassis link

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 35 on page 61.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 61.

Table 35: Configuring SNMP Views

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	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
Create a view.	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: set view *view-name*
Configure the view to include a MIB—for example, pingMIB.	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: set view *view-name* oid 1.3.6.1.2.1.80 include
Configure the view to exclude a MIB—for example, jnxPingMIB.	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: set view *view-name* oid jnxPingMIB exclude
Associate the view with a community.	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: set community *community-name* view *view-name*

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 show snmp statistics command.

```
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
```

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

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

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

Verifying SNMP Health Monitor Configuration

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

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

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

Alarm
Index  Variable description                           Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                         70 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                          0 active

 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                           20 active

 32772 Health Monitor: RE 0 memory utilization
       jnxOperatingBuffer.9.1.0.0                        95 rising threshold

 32774 Health Monitor: jkernel daemon memory usage
       Init daemon                                      912 active
       Chassis daemon                                 93356 active
       Firewall daemon                                 2244 active
```

```
       Interface daemon                              3340 active
       SNMP daemon                                   4412 active
       MIB2 daemon                                   3920 active
       VRRP daemon                                   2724 active
       Alarm daemon                                  1868 active
       PFE daemon                                    2656 active
       CRAFT daemon                                  2064 active
       Traffic sampling control daemon               3320 active
       Remote operations daemon                      3020 active
       CoS daemon                                    3044 active
       Inet daemon                                   1304 active
       Syslog daemon                                 1344 active
       Web management daemon                         3264 active
       USB Supervise Daemon                          1100 active
       PPP daemon                                    2076 active
       DLSWD daemon                                 10240 active

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

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

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

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

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

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

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

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.

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

Chapter 4

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

Before configuring the DHCP server on J-series Services Routers, become familiar with the terms defined in Table 36 on page 66.

Table 36: 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, *DHCP Options and BOOTP Vendor Extensions*.
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, *Dynamic Host Configuration Protocol (DHCP)*.
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.

(To configure autoinstallation, see “Configuring Autoinstallation” on page 83.)

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 8 on page 69 through Figure 10 on page 71 show the DHCP Quick Configuration pages.

Figure 8: DHCP Quick Configuration Main Page

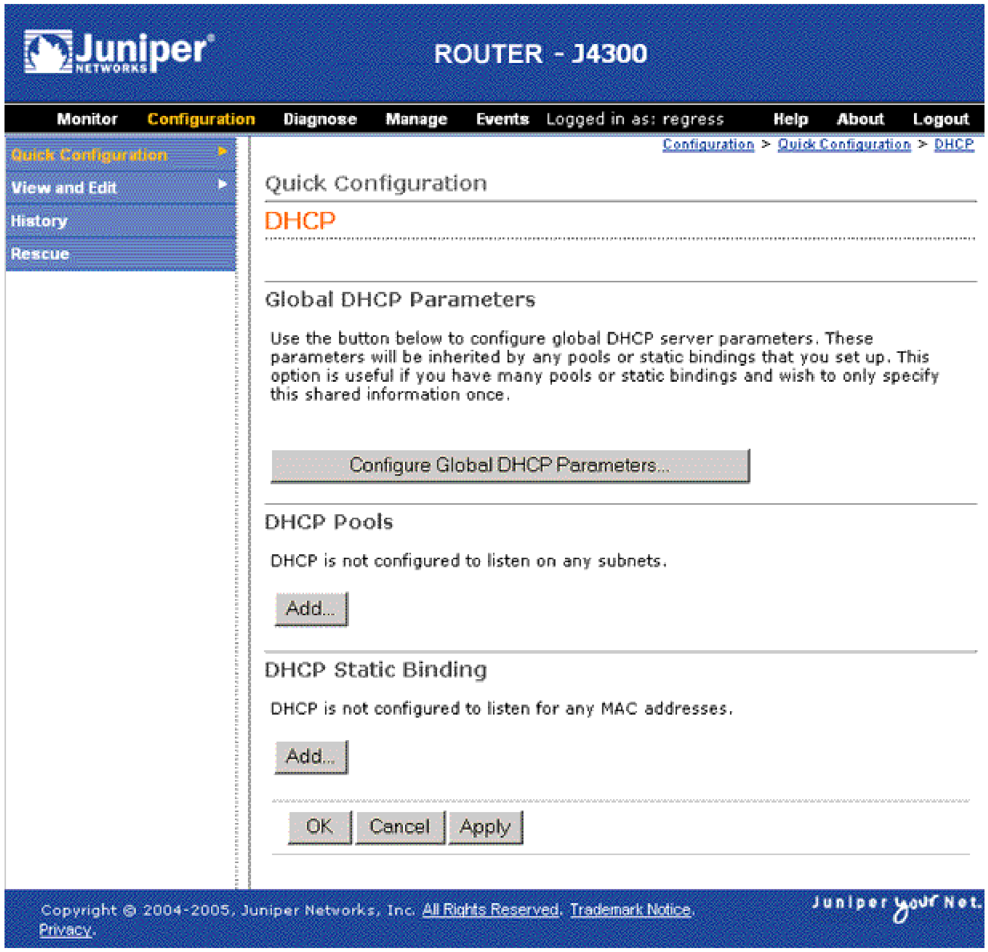


Figure 9: DHCP Quick Configuration Pool Page

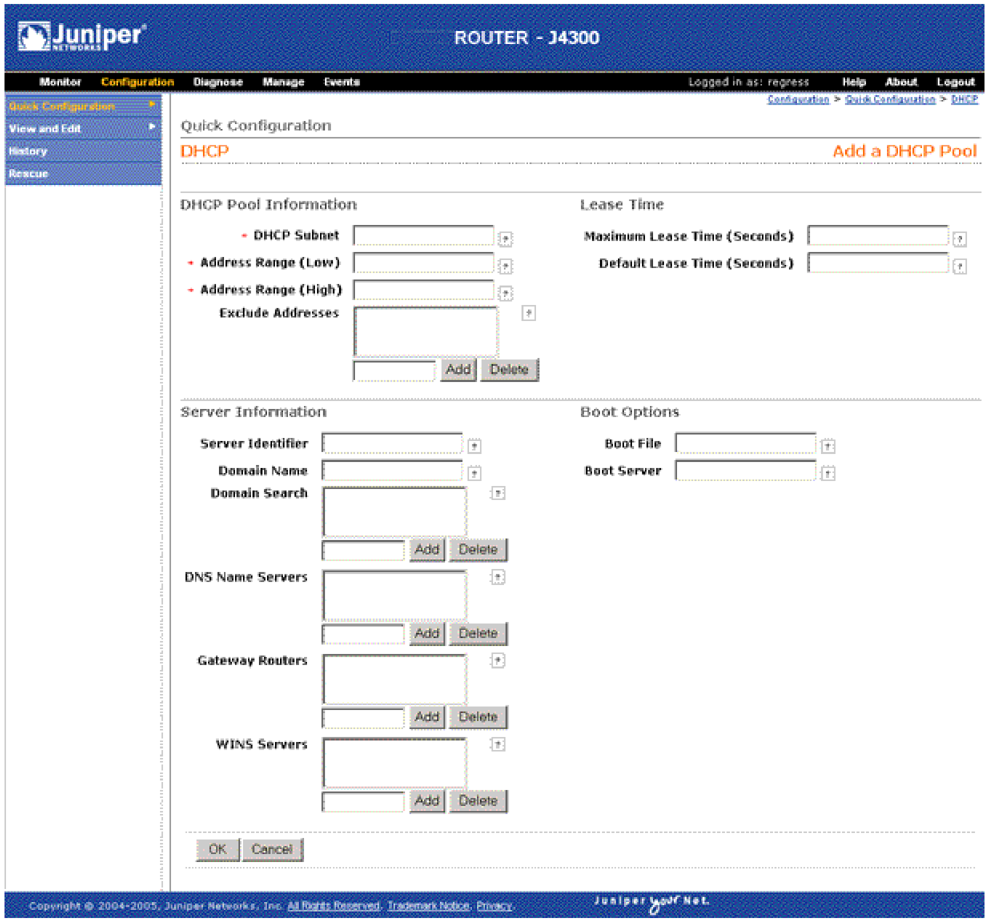
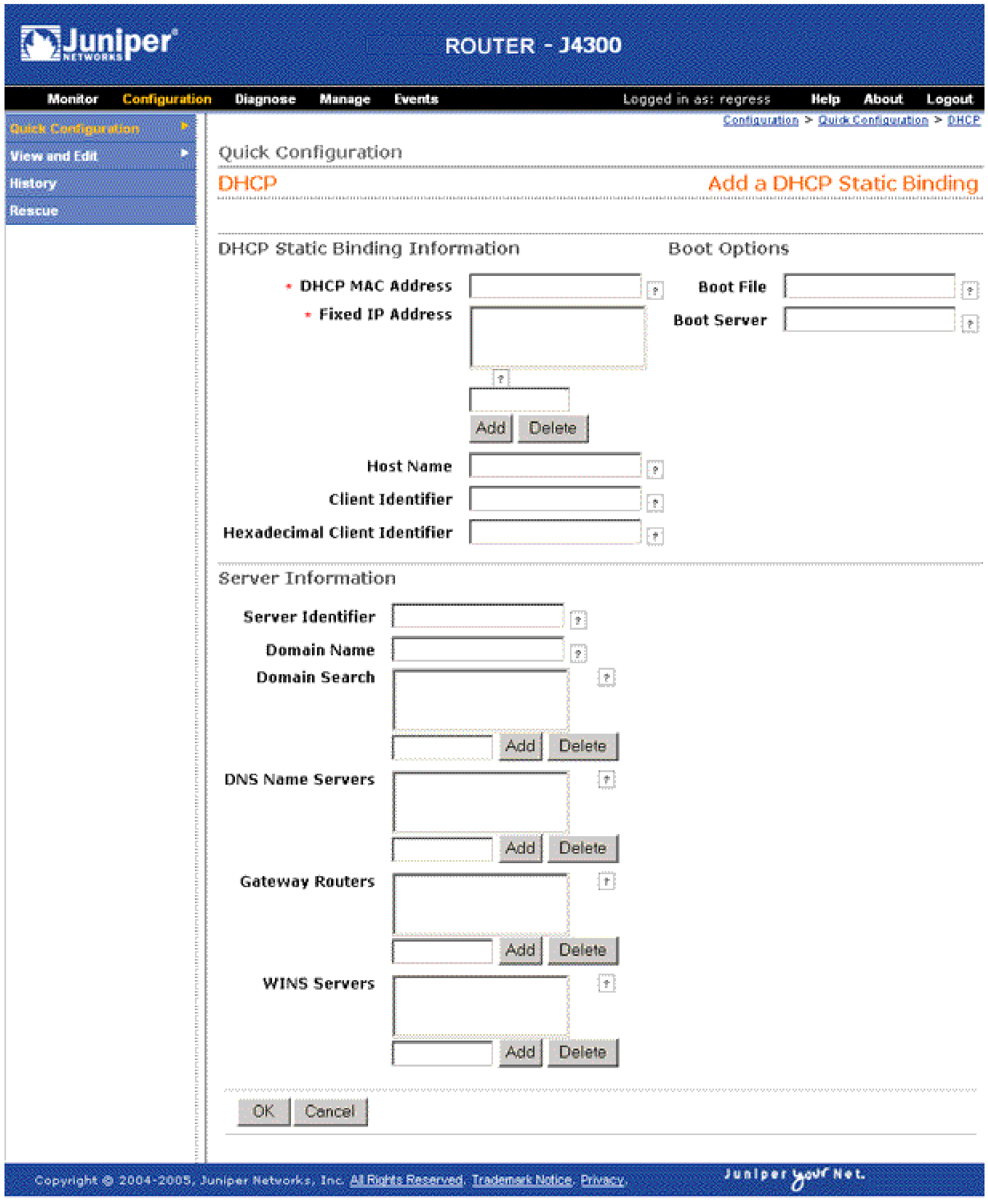


Figure 10: DHCP Quick Configuration Static Binding Page



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 37 on page 72.
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 77.
   - To verify DHCP operation, see "Verifying a DHCP Server Configuration" on page 77.

Table 37: 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).
Exclude Addresses	Specifies addresses to exclude from the IP address pool.	Do either of the following: ■ 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 least 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 least that never expires.
Server Information		

Table 37: DHCP Server Quick Configuration Pages Summary *(continued)*

Field	Function	Your Action
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: ■ 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: ■ 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: ■ To add a relay agent, type an IP address next to the **Add** button, and click **Add**. ■ To remove a relay agent, select the IP address in the Gateway Routers box, and click **Delete**.
WINS Servers	Defines a list of NetBIOS name servers, in order of preference—from top to bottom.	Do either of the following: ■ 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.

Table 37: DHCP Server Quick Configuration Pages Summary *(continued)*

Field	Function	Your Action
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: ■ 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 38 on page 74 provides the settings and values for the sample DHCP server configuration used in this section.

Table 38: Sample DHCP Server Configuration Settings

Settings	Sample Value or Values
DHCP Subnet Configuration	

Table 38: Sample DHCP Server Configuration Settings *(continued)*

Settings	Sample Value or Values
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 39 on page 76.
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 77.

Table 39: Configuring the DHCP Server

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Dhcp server** level in the configuration hierarchy.	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.	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.	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.	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
Exclude addresses from the IP address pool.	1. Next to Exclude address, click **Add new entry**. 2. In the Address box, type 192.168.2.33. 3. Click **OK**.	Set the address to exclude from the IP address pool: set pool 192.168.2.0/24 exclude-address 192.168.2.33

Table 39: Configuring the DHCP Server *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Define a DNS server.	1. Next to Name server, click **Add new entry**. 2. In the Address box, type 192.168.10.2. 3. Click **OK**.	Set the DNS server IP address: set pool 192.168.2.0/24 name-server 192.168.10.2
Define DHCP option 32—the router solicitation address option.	1. Next to Option, click **Add new entry**. 2. In the Option identifier code box, type 32. 3. From the Option type choice list, select **Ip address**. 4. In the Ip address box, type 192.168.2.33. 5. Click **OK** twice.	Set the router solicitation IP address: set pool 192.168.2.0/24 option 32 ip-address 192.168.2.33
Assign a static IP address of 192.168.2.50 to MAC address 01:03:05:07:09:0B.	1. Next to Static binding, click **Add new entry**. 2. In the Mac address box, type 01:03:05:07:09:0B. 3. Next to Fixed address, click **Add new entry**. 4. In the Address box, type 192.168.2.50. 5. Click **OK** until you return to the Configuration page.	Associate a fixed IP address with the MAC address of the client: set static-binding 01:03:05:07:09:0B fixed-address 192.168.2.50

Verifying a DHCP Server Configuration

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

- Displaying a DHCP Server Configuration on page 77
- Verifying the DHCP Binding Database on page 78
- Verifying DHCP Server Operation on page 79
- Displaying DHCP Statistics on page 81

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.

```
[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.

Related Topics 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 74 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 145.

```
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.

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

Verifying DHCP Server Operation

Purpose Verify that the DHCP server is operating as configured.

Action Take the following actions:

- Use the ping command to verify that a client responds to ping packets containing the destination IP address assigned by the 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.

```
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.
- 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 74, 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.

Related Topics To use the J-Web interface to ping a host, see "Using the J-Web Ping Host Tool" on page 226. For more information about the ping command, see "Pinging Hosts from the CLI" on page 244 or the *JUNOS System Basics and Services Command Reference*.

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.

```
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.

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

Chapter 5
Configuring Autoinstallation

If you are setting up many J-series Services Routers, autoinstallation can help automate the configuration process by loading configuration files onto new or existing routers automatically over the network. You can use either the J-Web configuration editor or CLI configuration editor to configure a Services Router for autoinstallation. The J-Web interface does not include Quick Configuration pages for autoinstallation.

This chapter contains the following topics:

Autoinstallation Terms

Before configuring autoinstallation, become familiar with the terms defined in Table 40 on page 83.

Table 40: Autoinstallation Terms

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

Table 40: Autoinstallation Terms *(continued)*

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

Autoinstallation Overview

Autoinstallation provides automatic configuration for a new Services Router that you connect to the network and turn on, or for a Services Router configured for autoinstallation. The autoinstallation process begins anytime a Services Router is powered on and cannot locate a valid configuration file in the compact flash. Typically, a configuration file is unavailable when a Services Router is powered on for the first time, or if the configuration file is deleted from the compact flash. The autoinstallation feature enables you to deploy multiple Services Routers from a central location in the network.

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

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

This overview contains the following topics:

- Supported Autoinstallation Interfaces and Protocols on page 84
- Typical Autoinstallation Process on a New Services Router on page 85

Supported Autoinstallation Interfaces and Protocols

Before autoinstallation on a Services Router can take place, the router must acquire an IP address. The protocol or protocols you choose for IP address acquisition determine the router interface to connect to the network for autoinstallation. The router detects the connected interface and requests an IP address with a protocol appropriate for the interface. Autoinstallation is supported over an Ethernet LAN interface or a serial LAN or WAN interface. Table 41 on page 85 lists the protocols that the router can use on these interfaces for IP address acquisition.

Table 41: Interfaces and Protocols for IP Address Acqusition During Autoinstallation

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

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

Typical Autoinstallation Process on a New Services Router

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

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

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

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

     If the DHCP server provides only the hostname, a DNS server must be available on the network to resolve the name to an IP address.
   - The IP address of an intermediate router if the configuration server is on a different LAN segment from the new router.

2. After the new Services Router acquires an IP address, the autoinstallation process on the router attempts to download a configuration file in the following ways:

a. If the DHCP server specifies the host-specific configuration file (boot file) *hostname*.conf, the router uses that filename in the TFTP server request. (In the filename, *hostname* is the hostname of the new router.) The autoinstallation process on the new router makes three unicast TFTP requests for *hostname*.conf. If these attempts fail, the router broadcasts three requests to any available TFTP server for the file.

b. If the new router cannot locate *hostname*.conf, the autoinstallation process unicasts or broadcasts TFTP requests for a default router configuration file called network.conf, which contains hostname-to-IP address mapping information, to attempt to find its hostname.

c. If network.conf contains no hostname entry for the new Services Router, the autoinstallation process sends out a DNS request and attempts to resolve the new router's IP address to a hostname.

d. If the new Services Router can determine its hostname, it sends a TFTP request for the *hostname*.conf file.

e. If the new Services Router is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file router.conf.

3. After the new Services Router locates a configuration file on a TFTP server, autoinstallation downloads the file, installs the file on the router, and commits the configuration.

Before You Begin

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

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

  You can configure a Services Router to operate as a DHCP server. For more information, see “Configuring the Router as a DHCP Server” on page 65.

- Create one of the following configuration files, and store it on a TFTP server in the network:
  - A host-specific file with the name *hostname*.conf for each Services Router undergoing autoinstallation. Replace *hostname* with the name of a Services Router. The *hostname*.conf file typically contains all the configuration information necessary for the router with this hostname.
  - A default configuration file named router.conf with the minimum configuration necessary to enable you to telnet into the new Services Router for further configuration.

- Physically attach the Services Router to the network using one or more of the following interface types:
  - Fast Ethernet
  - Gigabit Ethernet

  - Serial with HDLC encapsulation

- If you configure the DHCP server to provide only the TFTP server hostname, add an IP address-to-hostname mapping entry for the TFTP server to the DNS database file on the DNS server in the network.
- If the new router is not on the same network segment as the DHCP server (or other device providing IP address resolution), configure an existing router as an intermediate to receive TFTP and DNS requests and forward them to the TFTP server and the DNS server. You must configure the LAN or serial interface on the intermediate router with the IP addresses of the hosts providing TFTP and DNS service. Connect this interface to the new router.
- If you are using *hostname*.conf files for autoinstallation of host-specific configuration files, you must also complete the following tasks:
  - Configure the DHCP server to provide a *hostname*.conf filename to each new Services Router. Each router uses its *hostname*.conf filename to request a configuration file from the TFTP server. Copy the necessary *hostname*.conf configuration files to the TFTP server.
  - Create a default configuration file named network.conf, and copy it to the TFTP server. This file contains IP address-to-hostname mapping entries. If the DHCP server does not send a *hostname*.conf filename to a new router, the Services Router uses network.conf to resolve its hostname based on its IP address.

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

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

Configuring Autoinstallation with a Configuration Editor

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

To configure autoinstallation:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 42 on page 88.
3. If you are using the J-Web interface, click **Commit** to view a summary of your changes, then click **OK** to commit the configuration. If you are using the CLI, commit the configuration by entering the commit command.
4. To check the configuration, see “Verifying Autoinstallation” on page 88.

Table 42: Configuring Autoinstallation

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	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
Enable autoinstallation.	Select **Autoinstallation**, and then click **Configure**.	Enter set autoinstallation configuration-servers *url*
Specify the URL address of one or more servers from which to obtain configuration files. For example: ■ tftp://tftpconfig.sp.com ■ ftp://*user*:*password* @sftpconfig.sp.com	1. Next to Configuration servers, click **Add new entry**. 2. Type the location of the configuration server in the Url box. 3. If a password is required for server access, type it into the Password box. 4. Click **OK** to return to the Autoinstallation page.	
Configure one or more Ethernet or serial interfaces to perform autoinstallation.	1. Next to Interfaces, click **Add new entry**. 2. Type the name of the interface into the Interface name box—for example, ge-0/0/0. 3. Click **OK**.	To set BOOTP and RARP on an Ethernet interface, enter set autoinstallation interfaces ge-0/0/0 bootp rarp
Configure one or two procurement protocols for each interface. The router uses the protocols to send a request for an IP address for the interface. ■ BOOTP—Sends requests over all interfaces. ■ RARP—Sends requests over Ethernet interfaces. ■ SLARP—Sends requests over serial interfaces.	1. Next to the interface name, click **Edit**. 2. Select one or two protocols to be used by autoinstallation over the interface—for example, **Bootp** and **Rarp**. 3. Click **OK**.	

Verifying Autoinstallation

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

Verifying Autoinstallation Status

Purpose Display the status of the autoinstallation feature on a Services Router.

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

```
user@host> show system autoinstallation status
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  State: Configuration Acquisition
  Acquired:
    Address: 192.168.124.75
    Hostname: host-ge-000
    Hostname source: DNS
    Configuration filename: router-ge-000.conf
    Configuration filename server: 10.25.100.3
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
Interface:
  Name: ge-0/0/1
  State: None
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

What It Means The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the Services Router when it is deployed on the network.

Chapter 6

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*.

If the router is operating in a Common Criteria environment, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

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

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 43 on page 93.
5. If you are finished configuring the network, commit the configuration.

Table 43: Enabling Commit Scripts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Commit** level in the configuration hierarchy.	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 edit system scripts commit
Enable the commit script file—for example, commit-script.xsl.	1. Next to File, click **Add new entry**. 2. In the File name box, type commit-script.xsl. 3. Click **OK**.	Set the script file name: set file commit-script.xsl

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 reenable the script as described in “Enabling Commit Scripts” on page 92. 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.xsl
```

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.xsl
```

2. Commit the configuration:

```
user@host# commit
```

```
commit complete
```

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

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 96.

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 44 on page 95.
5. If you are finished configuring the network, commit the configuration.

Table 44: Enabling Operation Scripts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Op** level in the configuration hierarchy.	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 edit system scripts op
Enable the operation script file—for example, op-script.xsl.	1. Next to File, click **Add new entry**. 2. In the Name box, type op-script.xsl. 3. Click **OK**.	Set the script file name: set file op-script.xsl

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 96.

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 95. 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 97
- Configuring Event Policies on page 97

Event Policy Overview

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

- Ignore the event—Do not generate a system log message for this event and do not process any further policy instructions for this event.
- Raise a trap—Initiate an SNMP trap to notify SNMP trap-based applications when the event occurs.
- Upload a file—Upload a file to a specified destination. You can specify a transfer delay, so that, on receipt of an event, the upload process begins after the configured transfer delay. For example, a transfer delay can ensure that a core file has been completely generated before being uploaded.
- Execute CLI operational mode commands—Execute commands when an event occurs. The output of these commands is stored in a file, which is then uploaded to a specified URL.
- Execute operation scripts—Execute operation scripts when an event occurs. The output of the operation scripts is stored in a file, which is then uploaded to a specified URL. For information about operation scripts, see "Automating Network Management and Troubleshooting with Operation Scripts" on page 94.

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 45 on page 98.
3. If you are finished configuring the network, commit the configuration.

Table 45: 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.	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/.	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		
Navigate to the **Policy** level in the configuration hierarchy, and enter the policy name—for example, event1.	1. On the main Configuration page next to Event options, click **Configure** or **Edit**. 2. Next to Policy, click **Add new entry**. 3. In the Policy name box, type event1.	From the [edit] hierarchy level, enter edit event-options policy event1
Configure the event name—for example, SNMP_TRAP_LINK_DOWN. The SNMP_TRAP_LINK_DOWN event occurs when an interface that is monitored by SNMP becomes unavailable.	1. Next to Events, click **Add new entry**. 2. In the Event box, type SNMP_TRAP_LINK_DOWN. 3. Click **OK**.	Set the event name: set events SNMP_TRAP_LINK_DOWN

Table 45: Configuring Event Policies *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Flag the event to initiate an SNMP trap when it generates a system log message.	1. Next to Then, click **Configure**. 2. Select the **Raise trap** checkbox. 3. Click **OK**.	Enter set then set raise-trap
Define the action to be taken when the configured event occurs. For example, configure the Services Router to do the following when the SNMP_TRAP_LINK_DOWN event occurs for the t1–3/0/0 interface: 1. Execute the show interfaces t1–3/0/0 and show configuration interfaces t1–3/0/0 commands. 2. Upload the output of the show commands in a text file named config.txt to a server named bsd2. **NOTE:** Do not include spaces, the slash, or the percent sign (%) in the filename.	1. Next to Attributes match, click **Add new entry**. 2. In the Condition list, select **matches**. 3. In the From event attribute box, type SNMP_TRAP_LINK_DOWN.interface-name. 4. In the To event attribute value box, type t1–3/0/0. 5. Click **OK**. 6. Next to Then, click **Configure**. 7. Next to Execute commands, click **Configure**. 8. In the Destination box, type bsd2. 9. In the Output filename box, type config.txt. 10. From the Output format list, select **text**. 11. Next to Commands, click **Add new entry**. 12. In the Command box, type show interfaces t1–3/0/0. 13. Click **OK**. 14. Next to Commands, click **Add new entry**. 15. In the Command box, type show configuration interfaces t1–3/0/0. 16. Click **OK**.	1. Set the condition to execute the event policy only when the SNMP_TRAP_LINK_DOWN event occurs for the t1–3/0/0 interface: set attributes-match SNMP_TRAP_LINK_DOWN.interface-name equals t1–3/0/0 2. Enter edit then execute-commands 3. Set the commands to be executed when the configured event occurs: set commands show interfaces t1–3/0/0 set commands show configuration interfaces t1–3/0/0 4. Set the name and format of the file in which the output of the executed commands is to be uploaded to a destination server: set output-filename config.txt output-format text 5. Set the name of the server to which the file containing the command output is to be uploaded: set destination bsd2

Part 2

Monitoring a Services Router

Chapter 7

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

Before monitoring J-series Services Routers, become familiar with the terms defined in Table 46 on page 103.

Table 46: 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

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 47 on page 104 explains what each J-Web Monitor option displays and lists the corresponding CLI show commands.

Table 47: J-Web Monitor Options and Corresponding 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 109.	■ show system uptime ■ show system users ■ show system storage ■ show system processes
Chassis	Displays active chassis alarms, environment and hardware information, and status of Physical Interface Modules (PIMs). For details, see "Monitoring the Chassis" on page 113.	■ show chassis alarms ■ show chassis environment ■ show chassis fpc ■ show chassis hardware
Interfaces	Hierarchically displays all Services Router physical and logical interfaces, including state and configuration information. For details, see "Monitoring the Interfaces" on page 115.	■ show interfaces terse ■ show interfaces detail ■ show interfaces *interface-name*

Table 47: J-Web Monitor Options and Corresponding CLI show Commands *(continued)*

Monitor Option	Function	Corresponding CLI Commands
Routing	Displays routing information through the following options: ■ 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. For details, see “Monitoring Routing Information” on page 117.	■ Route information ■ show route terse ■ show route detail ■ OSPF information ■ show ospf neighbors ■ show ospf interfaces ■ show ospf statistics ■ BGP information ■ show bgp summary ■ show bgp neighbor ■ RIP information ■ show rip statistics ■ show rip neighbors ■ DLSw information ■ show dlsw capabilities ■ show dlsw circuits ■ show dlsw peers ■ show dlsw reachability
Class of Service (CoS)	Displays information about the performance of class of service on a router through the following options: ■ 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. For details, see “Monitoring Class-of-Service Performance” on page 125.	■ 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 47: J-Web Monitor Options and Corresponding 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—Information about the interfaces on which MPLS is enabled, including operational state and any administrative groups applied to an interface. ■ 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—Statistics for LSP sessions currently active on the Services Router, including the total number of packets and bytes forwarded through an LSP. ■ 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—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 132.	■ Interfaces—show mpls interface ■ LSP information—show mpls lsp ■ LSP Statistics—show mpls lsp statistics ■ RSVP Sessions—show rsvp session ■ RSVP Interfaces—show rsvp interface
Service Sets	Displays information about configured service sets. For details, see “Monitoring Service Sets” on page 137.	■ show services service-sets summary ■ show services service-sets memory-usage

Firewall	Displays firewall and intrusion detection service (IDS) information through the following options:
	■ Stateful Firewall—Displays the stateful firewall configuration.
	■ IDS Information—Displays information about the configured IDS.
	
	For details, see “Monitoring Firewalls” on page 138.
		■ Stateful firewall information
		  ■ show services stateful-firewall conversations
		  ■ show services stateful-firewall flows
		■ IDS information
		  ■ show services ids destination-table
		  ■ show services ids source-table
		  ■ show services ids pair-table

IPSec	Displays configured IPSec tunnels and statistics, and IKE security associations. For details, see “Monitoring IPSec Tunnels” on page 142.	■ show services ipsec-vpn ipsec statistics ■ show services ipsec-vpn ipsec security-associations ■ show services ipsec-vpn ike security-associations
NAT	Displays configured NAT pools. For details, see “Monitoring NAT Pools” on page 144.	■ show services nat pool

Table 47: J-Web Monitor Options and Corresponding CLI show Commands *(continued)*

Monitor Option	Function	Corresponding CLI Commands
DHCP	Displays DHCP dynamic and static leases, conflicts, pools, and statistics. For details, see "Monitoring DHCP" on page 145.	■ show system services dhcp binding ■ show system services dhcp conflict ■ show system services dhcp pool ■ show system services dhcp statistics
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 147.	show services rpm probe-results
PPPoE	Displays the following PPPoE information: ■ PPPoE Interfaces—Session-specific information about the interfaces on which PPPoE is enabled. ■ PPPoE Statistics—Statistics for PPPoE sessions currently active. ■ PPPoE Version—Information about the PPPoE protocol currently configured on the router. For details, see "Monitoring PPPoE" on page 150.	■ PPPoE interfaces—show pppoe interfaces ■ PPPoE statistics—show pppoe statistics ■ PPPoE version—show pppoe version
Media Gateway	Displays the following TGM550 Media Gateway information: ■ Dynamic Call Admission Control Information—Displays maximum bandwidth available for voice traffic and the dynamic call admission control (CAC) properties configured on the router WAN interfaces. ■ Telephony Gateway Module Information—Displays information about TGM550 connectivity and digital signal processor (DSP) capacity. ■ Telephony Interface Module Information—Displays the online and offline status of telephony interface modules (TIMs) installed in a J-series router. For details, see "Monitoring the TGM550 Media Gateway (VoIP)" on page 153.	■ Dynamic call admission control information—show tgm dynamic-call-admission-control ■ Telephony Gateway Module information—show tgm fpc *slot-number* media-gateway-controller and show tgm fpc *slot-number* dsp-capacity ■ Telephony Gateway Module status—show tgm telephony-interface-module status

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 13 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

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 48 on page 109 summarizes key output fields in system properties displays.

Table 48: Summary of Key System Properties Output Fields

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

Table 48: 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 (ge-0/0/0, for example), as defined with the set interfaces ge-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.

Table 48: Summary of Key System Properties Output Fields *(continued)*

Field	Values	Additional Information
Memory Usage		
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 show system processes 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 restart 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 show system processes 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 restart command from the CLI.
CPU Usage	Percentage of the CPU that is being used by the process.	

Table 48: Summary of Key System Properties Output Fields *(continued)*

Field	Values	Additional Information
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.	
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 /var/log 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 /var/tmp 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 /var/crash 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 /var/db 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 49 on page 112 summarizes the output fields in the system process information display.

Table 49: 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.	

Table 49: Summary of System Process Information Output Fields *(continued)*

Field	Values	Additional Information
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 active chassis alarms on the Services Router, environment measurements, a summary of the field-replaceable units (FRUs), and the status of Physical Interface Modules (PIMs) 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 fpc
- show chassis hardware

CAUTION: Do not install a combination of PIMs in a single chassis that exceeds the maximum power and heat capacity of the chassis. If J-series power management is enabled, PIMs that exceed the maximum power and heat limits remain offline when the chassis is powered on. To check PIM power and heat status, use the show chassis fpc and show chassis power-ratings commands. For more information, see the Getting Started Guide for your router.

Table 50 on page 113 summarizes key output fields in chassis displays.

Table 50: Summary of Key Chassis Output Fields

Field	Values	Additional Information
Alarm Summary		
Alarm Time	Date and time the alarm was first recorded.	

Table 50: Summary of Key Chassis Output Fields *(continued)*

Field	Values	Additional Information
Alarm Class	Severity class for this alarm: Minor or Major.	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. Configurable alarms are set in either of the following ways: ■ 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 For details, see "Configuring and Monitoring Alarms" on page 169.
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 fans.	
Gauge Status	Status of the temperature gauge on the specified hardware component.	
Temperature	Temperature of the air flowing past the hardware component.	
Fan Status	Status of the fans that are regulated by the JUNOS software: ■ OK ■ Testing (when the router is powered on) ■ Failed ■ Absent	
Fan Speed	Speed of the fans: normal or high speed.	Speed is adjusted automatically according to the current temperature.
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.
Version	Revision level of the specified hardware component.	Supply the version number when reporting any hardware problems to customer support.

Table 50: Summary of Key Chassis Output Fields *(continued)*

Field	Values	Additional Information
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.
FPC Summary		
Slot	FPC or PIM slot number.	On J-series Services Routers, an FPC and a PIM are the same physical unit.
State	State of the slot: ■ Dead—Held in reset because of errors. ■ Diag—Slot is being ignored while the FPC or PIM is running diagnostics. ■ Dormant—Held in reset. ■ Empty—No FPC or PIM is present. ■ Online—FPC or PIM is online and running. ■ Probed—Probe is complete. The FPC is awaiting restart of the Packet Forwarding Engine (PFE). ■ Probe-wait—The FPC is waiting to be probed.	
Temp (C)	Temperature of the air passing by the FPC, in degrees Celsius.	J-series Services Routers do not monitor and report the temperature of PIMs.
CPU Utilization (%)	Total—Total percentage of CPU being used by the FPC or PIM processor. Interrupt—Of the total CPU being used by the FPC or PIM processor, the percentage being used for interrupts.	
Memory DRAM (MB)	Total DRAM, in megabytes, available to the FPC or PIM processor.	
Utilization (%)	Heap—Percentage of heap space (dynamic memory) being used by the FPC or PIM processor. Buffer—Percentage of buffer space being used by the FPC or PIM processor for buffering internal messages.	If the heap space utilization exceeds 80 percent, a memory leak might be occurring.

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 51 on page 116 summarizes key output fields in interfaces displays.

Table 51: Summary of Key Interfaces Output Fields

Field	Values	Additional Information
Interface Summary		
Interface Name	Name of interface. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	Click an interface name to see more information about the interface. Channelized interfaces appear as two interfaces, which can both be monitored. For example: ■ If ce1-3/0/0 is configured as a clear channel, you can monitor ce1-3/0/0 and e1-3/0/0. ■ If ct1-3/0/1 is channelized, you can monitor ct1-3/0/1 and ds-3/0/1:1.
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.
Admin State	Whether the interface is enabled up (Up) or disabled (Down).	Interfaces are enabled by default. To disable an interface: ■ 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 *interfaces-name*] level of the configuration hierarchy
Description	Configured description for the interface.	
Interface: *interface-name*		
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 51: Summary of Key Interfaces Output Fields *(continued)*

Field	Values	Additional Information
Admin State	Whether the interface is enabled up (Up) or disabled (Down).	Interfaces are enabled by default. To disable an interface: ■ 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 *interfaces-name*] 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.	Configure alarms on interfaces as follows: ■ 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.	
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 Route Information

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 52 on page 118 summarizes key output fields in the routing information display.

Table 52: Summary of Key Routing Information Output Fields

Field	Values	Additional Information
n destinations	Number of destinations for which there are routes in the routing table.	
n routes	Number of routes in the routing table: ■ 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.

Table 52: Summary of Key Routing Information Output Fields *(continued)*

Field	Values	Additional Information
Next-Hop	Network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.	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. 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. 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).
Age	How long the route has been known.	
State	Flags for this route.	There are many possible flags. For a complete description, see the *JUNOS Interfaces Command Reference*.
AS Path	AS path through which the route was learned. The letters of the AS path indicate the path origin: ■ 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 53 on page 119 summarizes key output fields in the BGP routing display.

Table 53: Summary of Key BGP Routing Output Fields

Field	Values	Additional Information
BGP Summary		
Groups	Number of BGP groups.	
Peers	Number of BGP peers.	

Table 53: Summary of Key BGP Routing Output Fields *(continued)*

Field	Values	Additional Information
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. ■ If a peer is not established, the field shows the state of the peer session: Active, Connect, or Idle. ■ If a BGP session is established, the field shows the number of active, received, and damped routes that are received from a neighbor. For example, 2/4/0 indicates two active routes, four received routes, and no damped routes.	
BGP Neighbors		
Peer	Address of the BGP neighbor.	
AS	AS number of the peer.	
Type	Type of peer: Internal or External.	
State	Current state of the BGP session: ■ 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.	Generally, the most common states are Active, which indicates a problem establishing the BGP conenction, 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.

Table 53: Summary of Key BGP Routing Output Fields *(continued)*

Field	Values	Additional Information
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 54 on page 121 summarizes key output fields in the OSPF routing display.

Table 54: 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.

Table 54: Summary of Key OSPF Routing Output Fields *(continued)*

Field	Values	Additional Information
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.	
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 55 on page 122 summarizes key output fields in the RIP routing display.

Table 55: 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.	

Table 55: Summary of Key RIP Routing Output Fields *(continued)*

Field	Values	Additional Information
Routes advertised	Number of RIP routes advertised on the logical interface.	
RIP Neighbors		
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. The name is set in either of the following ways: ■ In the J-Web configuration editor, on the **Protocols > RIP > Group >** *group-name* **> Neighbor** page ■ In the CLI configuration editor, with the neighbor *neighbor-name* statement at the [edit protocols rip group *group-name*] level of the configuration hierarchy
State	State of the RIP connection: Up or Dn (Down).	
Source Address	Local source address.	This value is the configured address of the interface on which RIP is enabled.
Destination Address	Destination address.	This value is the configured address of the immediate RIP adjacency.
In Met	Value of the incoming metric configured for the RIP neighbor.	

Monitoring 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 56 on page 123 summarizes key routing information output fields in the DLSw routing display.

Table 56: 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.	

Table 56: Summary of Key DLSw Routing Information Output Fields *(continued)*

Field	Values	Additional Information
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.	
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 inital pacing frame.	
No circuits timeout	Length of time before a circuit becomes inactive.	

Table 56: Summary of Key DLSw Routing Information Output Fields *(continued)*

Field	Values	Additional Information
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

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 57 on page 126 summarizes key output fields for CoS interfaces.

Table 57: 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.	
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 58 on page 126 summarizes key output fields for CoS classifiers.

Table 58: Summary of Key CoS Classifier Output Fields

Classifier Name	Name of a classifier.	To display classifier assignments, click the plus sign (+).

Table 58: Summary of Key CoS Classifier Output Fields *(continued)*

CoS Value Type	The classifiers are displayed by type: ■ 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 59 on page 128 summarizes key output fields for CoS value aliases.

Table 59: Summary of Key CoS Value Alias Output Fields

Field	Values	Additional Information
CoS Value Type	Type of the CoS value: ■ 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 60 on page 128 summarizes key output fields for CoS RED drop profiles.

Table 60: 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.

Table 60: Summary of Key CoS RED Drop Profile Output Fields *(continued)*

Field	Values	Additional Information
Type	Type of a specific drop profile: ■ 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 *JUNOS Class of Service Configuration Guide*.	
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 61 on page 130 summarizes key output fields for CoS forwarding classes.

Table 61: Summary of Key CoS Forwarding Class Output Fields

Field	Values	Additional Information
Forwarding Class	Names of forwarding classes assigned to queue numbers. By default, the following forwarding classes are assigned to queues 0 through 3: ■ 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 62 on page 130 summarizes key output fields for CoS rewrite rules.

Table 62: Summary of Key CoS Rewrite Rules Output Fields

Field	Values	Additional Information
Rewrite Rule Name	Names of rewrite rules.	
CoS Value Type	Rewrite rule type: ■ dscp—For IPv4 DiffServ traffic. ■ dscp-ipv6—For IPv6 DiffServ traffic. ■ exp—For MPLS traffic. ■ ieee-802.1—For Layer 2 traffic. ■ inet-precedence—For IPv4 traffic.	To display forwarding classes, loss priorities, and rewritten CoS values, click the plus sign (+).
Index	Internal index for this particular rewrite rule.	

Table 62: Summary of Key CoS Rewrite Rules Output Fields *(continued)*

Field	Values	Additional Information
Forwarding Class	Forwarding class that in combination with loss priority is used to determine CoS values for rewriting.	Rewrite rules are applied to CoS values in outgoing packets based on forwarding class and loss priority setting.
Loss Priority	Loss priority that in combination with forwarding class is used to determine CoS values for rewriting.	
Rewrite CoS Value To	Value that the CoS value is rewritten to.	

Monitoring CoS Scheduler Maps

To display assignments of CoS forwarding classes to schedulers, select **Monitor > Class of Service > Scheduler Maps** in the J-Web interface, or enter the following CLI command:

show class-of-service scheduler-map

Table 63 on page 131 summarizes key output fields for CoS scheduler maps.

Table 63: Summary of Key CoS Scheduler Maps Output Fields

Field	Values	Additional Information
Scheduler Map	Name of a scheduler map.	For details, click the plus sign (+).
Index	Index of a specific object—scheduler maps, schedulers, or drop profiles.	
Scheduler Name	Name of a scheduler.	
Forwarding Class	Forwarding classes this scheduler is assigned to.	
Transmit Rate	Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following: ■ A percentage—The scheduler receives the specified percentage of the total interface bandwidth. ■ remainder—The scheduler receives the remaining bandwidth of the interface after allocation to other schedulers.	
Rate Limit	Rate limiting configuration of the queue: ■ none—No rate limiting. ■ exact—The queue transmits at only the configured rate.	

Table 63: Summary of Key CoS Scheduler Maps Output Fields *(continued)*

Field	Values	Additional Information
Buffer Size	Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following: ■ A percentage—The buffer is a percentage of the total buffer allocation. ■ remainder—The buffer is sized according to what remains after other scheduler buffer allocations.	
Priority	Scheduling priority of a queue: ■ high—Packets in this queue are transmitted first. ■ low—Packets in this queue are transmitted last. ■ medium-high—Packets in this queue are transmitted after high-priority packets. ■ medium-low—Packets in this queue are transmitted before low-priority packets.	
Drop Profiles	Name and index of a drop profile that is assigned to a specific loss priority and protocol pair.	
Loss Priority	Packet loss priority corresponding to a drop profile: ■ 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 133
- Monitoring MPLS LSP Information on page 133

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 64 on page 133 summarizes key output fields in the MPLS interface information display.

Table 64: 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 65 on page 133 summarizes key output fields in the MPLS LSP information display.

Table 65: 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.

Table 65: Summary of Key MPLS LSP Information Output Fields *(continued)*

Field	Values	Additional 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.	
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 66 on page 135 summarizes key output fields in the MPLS LSP statistics display.

Table 66: 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.
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 67 on page 135 summarizes key output fields in the RSVP session information display.

Table 67: Summary of Key RSVP Session Information Output Fields

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

Table 67: Summary of Key RSVP Session Information Output Fields *(continued)*

Field	Values	Additional Information
Transit LSP	Information about transit RSVP sessions.	MPLS learns this information by querying RSVP, which holds all the transit and outbound session information.
To	Destination (outbound 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.	
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 68 on page 136 summarizes key output fields in the RSVP interfaces information display.

Table 68: Summary of Key RSVP Interfaces Information Output Fields

Field	Values	Additional Information
RSVP Interface	Number of interfaces on which RSVP is active. Each interface has one line of output.	
Interface	Name of the interface.	

Table 68: Summary of Key RSVP Interfaces Information Output Fields *(continued)*

Field	Values	Additional Information
State	State of the interface: ■ Disabled—No traffic engineering information is displayed. ■ Down—The interface is not operational. ■ Enabled—Displays traffic engineering information. ■ Up—The interface is operational.	
Active resv	Number of reservations that are actively reserving bandwidth on the interface.	
Subscription	User-configured subscription factor.	
Static BW	Total interface bandwidth, in bits per second (bps).	
Available BW	Amount of bandwidth that RSVP is allowed to reserve, in bits per second (bps). It is equal to (static bandwidth X subscription factor).	
Reserved BW	Currently reserved bandwidth, in bits per second (bps).	
Highwater mark	Highest bandwidth that has ever been reserved on this interface, in bits per second (bps).	

Monitoring 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 69 on page 138 summarizes key output fields in service sets displays.

Table 69: 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 sp-0/0/0.	
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		
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: ■ 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

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 70 on page 139 summarizes key output fields for stateful firewall filter statistics.

Table 70: 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	Number of packets matching rules defined in new flows: ■ Accept—Number of packets accepted. ■ Discards—Number of packets discarded. ■ Rejects—Number of packets rejected.
Existing flows	Number of packets matching rules defined in existing flows: ■ Accept—Number of packets accepted. ■ Discards—Number of packets discarded. ■ Rejects—Number of packets rejected.
Drops	Number of packets dropped due to the following match conditions: ■ 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. For more information about these match conditions, see the *J-series Services Router Advanced WAN Access Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

Table 70: Summary of Key Stateful Firewall Statistics Output Fields *(continued)*

Field	Values
Errors	Number of protocol errors detected: ■ 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. For a complete list of protocol errors that are counted, see the description of the show services stateful-firewall statistics command in the *JUNOS System Basics and Services Command Reference*.

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 71 on page 140 summarizes key output fields for stateful firewall filters.

Table 71: 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: ■ 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.

Table 71: Summary of Key Stateful Firewall Filters Output Fields *(continued)*

Field	Values
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 72 on page 141, and click **OK**.

Table 72: 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: ■ **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 73 on page 142 summarizes key output fields for stateful firewall filter intrusion detection.

Table 73: 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).
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 74 on page 142 summarizes key output fields in IPSec displays.

Table 74: 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.

Table 74: Summary of Key IPSec Output Fields *(continued)*

Field	Values
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.
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: ■ 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.

Table 74: Summary of Key IPSec Output Fields *(continued)*

Field	Values
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: ■ 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.
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 75 on page 145 summarizes key output fields in NAT displays.

Table 75: 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 76 on page 145 summarizes the output fields in DHCP displays.

Table 76: 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.	

Table 76: Summary of DHCP Output Fields *(continued)*

Field	Values	Additional Information
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 clear system services dhcp conflict 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.	
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.	

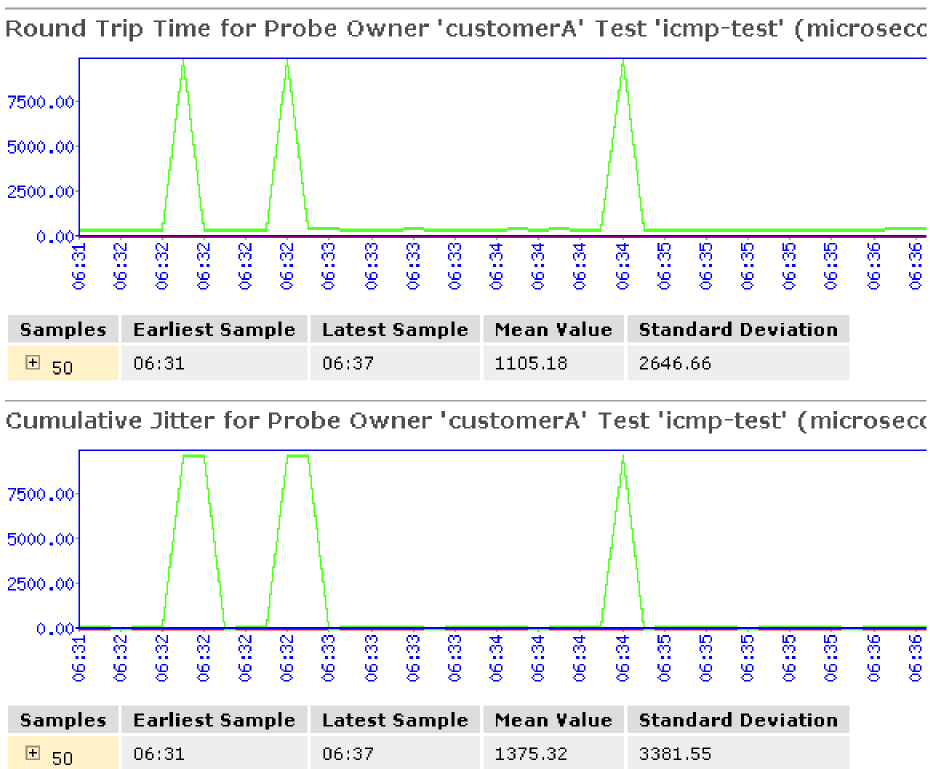
Monitoring RPM Probes

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 11 on page 147 shows sample graphs for an RPM test.

Figure 11: Sample RPM Graphs



In Figure 11 on page 147, 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 77 on page 147 summarizes key output fields in RPM displays.

Table 77: Summary of Key RPM Output Fields

Field	Values	Additional Information
Currently Running Tests		

Table 77: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Graph		Click the **Graph** link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	
Test Name	Configured name of the RPM test.	
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: ■ 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.

Table 77: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Earliest Sample	System time when the first probe in the sample was received.	
Latest Sample	System time when the last probe in the sample was received.	
Mean Value	Average round-trip time for the 50–probe sample.	
Standard Deviation	Standard deviation of the round-trip times for the 50–probe sample.	
Lowest Value	Shortest round-trip time from the 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.	

Table 77: Summary of Key RPM Output Fields *(continued)*

Field	Values	Additional Information
Time of Highest Sample	System time when the highest jitter value in the 50–probe sample was received.	

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 78 on page 151 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 115.

Table 78: Summary of Key PPPoE Output Fields

Field	Values	Additional Information
PPPoE Interfaces		
Interface	Name of the PPPoE interface. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	Click the interface name to display PPPoE information for the interface.
State	State of the PPPoE session on the interface.	
Session ID	Unique session identifier for the PPPoE session.	To establish a PPPoE session, first the 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, ge-0/0/0.1.	
PPPoE Statistics		
Active PPPoE Sessions	Total number of active PPPoE sessions.	

Table 78: Summary of Key PPPoE Output Fields *(continued)*

Field	Values	Additional Information
Packet Type	Packets sent and received during the PPPoE session, categorized by packet type and packet error: ■ 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	Information about the timeouts that occurred during the PPPoE session. ■ PADI—Number of timeouts that occurred for the PADI packet. ■ PADO—Number of timeouts that occurred for the PADO packet. (This value is always 0 and is not supported. ■ PADR—Number of timeouts that occurred for the PADR packet.	
Sent	Number of the timeouts that occurred for PADI, PADO, and PADR packets.	
PPPoE Version		
Maximum Sessions	Maximum number of active PPPoE sessions the Services Router can support. The default is 256 sessions.	

Table 78: Summary of Key PPPoE Output Fields *(continued)*

Field	Values	Additional Information
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.	

Monitoring the TGM550 Media Gateway (VoIP)

J4350 and J6350 Services Routers support voice over IP (VoIP) routing through an Avaya TGM550 Telephony Gateway Module and one or more Telephony Interface Modules (TIMs) installed in the router. From the J-Web interface or the JUNOS CLI, you can monitor the vp-*pim*/0/0 interface to the TGM550 (see "Monitoring the Interfaces" on page 115). In addition, you can monitor dynamic call admission control (CAC) operation, if it is configured on the router WAN interfaces, and also the list of Media Gateway Controllers (MGCs) configured on the TGM550.

To display TGM550 information, select **Monitor > Media Gateway** in the J-Web interface.

Alternatively, enter the following commands in the CLI operational mode:

- show tgm dynamic-call-admission-control
- show tgm fpc *slot-number* media-gateway-controller
- show tgm fpc *slot-number* dsp-capacity
- show tgm telephony-interace-module status

Table 79 on page 154 summarizes key output fields in media gateway information displays.

Table 79: Summary of Key Media Gateway Information Output Fields

Field	Values	Additional Information
Dynamic Call Admission Control Information		
Reported Bearer Bandwidth Limit	Maximum bandwidth available for voice traffic on the Services Router.	If dynamic CAC is configured on more than one active interface, the TGM550 reports the bearer bandwidth limit (BBL) of the active interface with the highest activation priority. If more than one active interface has the same activation priority, the BBL is reported as the number of those interfaces times their lowest BBL. For example if two interfaces with the same activation priority have BBLs of 2000 Kbps and 1500 Kbps, the RBBL is 3000 Kbps (2 x 1500 Kbps).
Interface Name	Name of interface on which dynamic CAC is configured. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	
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.
Activation Priority	Activation priority configured on the interface.	
Bearer Bandwidth Limit (Kbps)	Maximum bandwidth available for voice traffic on the interface.	
Telephony Gateway Module Information		
Media Gateway Controller (MGC) List	IP addresses of the MGCs configured in the MGC list for the TGM550.	
Slot state	Online and offline status of the telephony interface modules (TIMS)	
Offline Reason	Reason for offline status: Busy Out or Out of resources	

Table 79: Summary of Key Media Gateway Information Output Fields *(continued)*

Field	Values	Additional Information
DSP Capacity	Number of voice channels in the low capacity DSP	

Chapter 8

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*.

If the router is operating in a Common Criteria environment, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

System Log Message Terms

Before configuring and monitoring system log messages on Services Routers, become familiar with the terms defined in Table 80 on page 157.

Table 80: 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 81 on page 159.

Table 80: System Log Message Terms *(continued)*

<table>
<tr><th>Term</th><th>Definition</th></tr>
<tr><td>priority</td><td>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 JUNOS System Log Messages Reference. See also facility; severity level.</td></tr>
<tr><td>process</td><td>Software program, also known as a daemon, that controls router functionality. The following are some key JUNOS processes:

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.

For more information about processes, see the JUNOS Software Installation and Upgrade Guide.</td></tr>
<tr><td>process ID</td><td>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.</td></tr>
<tr><td>regular expressions</td><td>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 160.</td></tr>
<tr><td>severity level</td><td>Measure of how seriously a triggering event affects Services Router functions. For a list of severity levels that you can specify, see Table 82 on page 160.</td></tr>
</table>

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 162.
- 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 163.
- 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 81 on page 159 lists the system logging facilities, and Table 82 on page 160 lists the system logging severity levels. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Table 81: 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

Table 81: System Logging Facilities *(continued)*

Facility	Description
interactive-commands	Commands executed in the CLI
kernel	Messages generated by the JUNOS kernel
user	Messages from random user processes

Table 82: 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 83 on page 161 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 sytem log messages, see "Filtering System Log Messages" on page 165.

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

Table 83: Common Regular Expression Operators and the Terms They Match

<table>
<tr><th>Regular Expression Operator</th><th>Matching Terms</th></tr>
<tr><td>. (period)</td><td>One instance of any character except the space.

For example, .in matches messages with win or windows.</td></tr>
<tr><td>* (asterisk)</td><td>Zero or more instances of the immediately preceding term.

For example, tre* matches messages with tree, tread or trough.</td></tr>
<tr><td>+ (plus sign)</td><td>One or more instances of the immediately preceding term.

For example, tre+ matches messages with tree or tread but not trough.</td></tr>
<tr><td>? (question mark)</td><td>Zero or one instance of the immediately preceding term.

For example, colou?r matches messages with or color or colour.</td></tr>
<tr><td>| (pipe)</td><td>One of the terms that appear on either side of the pipe operator.

For example, gre|ay matches messages with either grey or gray.</td></tr>
<tr><td>! (exclamation point)</td><td>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.</td></tr>
<tr><td>^ (caret)</td><td>The start of a line, when the caret appears outside square brackets.

For example, ^T matches messages with This line and not with On this line.</td></tr>
<tr><td>$ (dollar sign)</td><td>Strings at the end of a line.

For example, :$ matches messages with the following: and not with 2:00.</td></tr>
<tr><td>[] (paired square brackets)</td><td>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, [0-9] matches messages with any number.</td></tr>
<tr><td>() (paired parentheses)</td><td>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, dev(/|ice) matches messages with dev/ or device.</td></tr>
</table>

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

You can direct system log messages to a file on the compact flash. The default directory for log files is /var/log. To specify a different directory on the compact flash, include the complete pathname. For the list of logging facilities and severity levels, see Table 81 on page 159 and Table 82 on page 160.

For information about archiving log files, see “Archiving System Logs” on page 163.

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 84 on page 162.
3. If you are finished configuring the network, commit the configuration.

Table 84: Sending System Log Messages to a File

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Syslog** level in the configuration hierarchy.	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.	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 81 on page 159 and Table 82 on page 160.

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 85 on page 163.
3. If you are finished configuring the network, commit the configuration.

Table 85: Sending Messages to a User Terminal

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Syslog** level in the configuration hierarchy.	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.	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

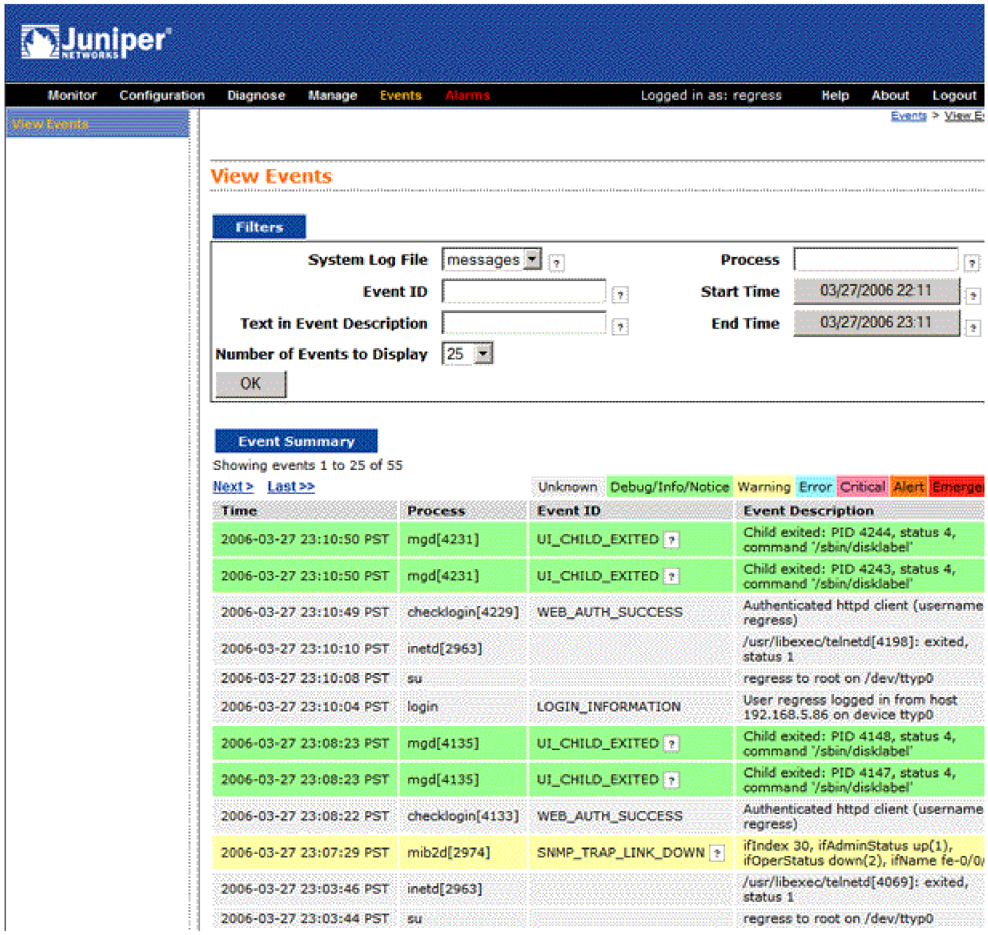
You can use the J-Web interface to filter and view system log messages on a Services Router. To view system log messages, click **Events** in the J-Web taskbar. (To view system log messages with the CLI, use the show log command.)

Figure 12 on page 165 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 165
- Viewing System Log Messages on page 167

Figure 12: View Events Page



Filtering System Log Messages

You can use filters to display relevant events. Table 86 on page 165 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 86: Filtering System Log Messages

Field	Function	Your Action
System Log File	Specifies the name of a system log file for which you want to display the recorded events. Lists the names of all the system log files that you configure. By default, a log file, messages, is included in the /var/log/ directory. For information about how to configure system log files, see "Sending System Log Messages to a File" on page 162.	To specify events recorded in a particular file, select the system log filename from the list—for example, **messages**.

Table 86: Filtering System Log Messages *(continued)*

Field	Function	Your Action
Event ID	Specifies the Event ID for which you want to display the messages. Allows you to type part of the ID and completes the remaining automatically. 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.	To specify events with a specific ID, type its partial or complete ID—for example, TFTPD_AF_ERR.
Text in Event Description	Specifies text from the description of events that you want to display. Allows you to use regular expression to match text from the event description. **NOTE:** The regular expression matching is case sensitive. For more information about using regular expressions, see "Regular Expressions" on page 160.	To specify events with a specific description, type a text string from the description with regular expression. For example, type ^Initial* to display all messages with lines beginning with the term *Initial*.
Process	Specifies the name of the process generating the events you want to display. To view all the processes running on your system, enter the CLI command—show system processes. For more information about processes, see the *JUNOS Software Installation and Upgrade Guide*.	To specify events generated by a process, type the name of the process. For example, type mgd to list all messages generated by the management process.
Start Time End Time	Specifies the time period in which the events you want displayed are generated. 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.	To specify the time period: ■ 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**. To select the current time as the start time, select **local time**.
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 87 on page 167 describes the Event Summary fields.

Table 87: 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.	
Event ID	Displays a code that uniquely identifies the message. The prefix on each code identifies the message source, and the rest of the code indicates the specific event or error. Displays context-sensitive help that provides more information about the event: ■ **Help**—Short description of the message. ■ **Description**—More detailed explanation of the message. ■ **Type**—Category to which the message belongs. ■ **Severity**—Level of severity.	The event ID begins with a prefix that indicates the generating software process. Some processes on a Services Router do not use codes. This field might be blank in a message generated from such a process. An Event can belong to one of the following Type categories: ■ **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.
Event Description	Displays a more detailed explanation of the message.	
Severity	Severity level of a message is indicated by different colors. ■ **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.	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.

Chapter 9

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

Before configuring and monitoring alarms on Services Routers, become familiar with the terms defined in Table 88 on page 169.

Table 88: 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 88: Alarm Terms *(continued)*

Term	Definition
interface alarm	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. 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. To enable an interface alarm, you must explicitly set an alarm condition.
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

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

Table 89 on page 172 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 89: 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	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 89: 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 89: 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 90 on page 175 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 90: 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.	Typically, the router boots from the internal compact flash. 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 xxi.)	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 185.) If this remedy fails, you must replace the failed Routing Engine. To contact JTAC, see “Requesting Support” on page xxi.	Yellow (minor)
	Routing Engine temperature is too warm.	■ Check the room temperature. (See the Getting Started Guide for your router.) ■ 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 xxi.) ■ If the router has an air filter, check the air filter and replace it if it appears clogged. (See the Getting Started Guide for your router.)	Yellow (minor)
	Routing Engine fan has failed.	Replace the failed fan. To contact JTAC, see “Requesting Support” on page xxi.	Red (major)

System Alarm Conditions and Corrective Actions

Table 91 on page 176 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 91: 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 *J-series Services Router Basic LAN and WAN Access Configuration Guide*.
License	You have configured at least one software feature that requires a feature license, but no valid license for the feature is currently installed. **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.	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 171.

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 92 on page 177.
3. If you are finished configuring the network, commit the configuration.
4. To verify the alarms configuration, see Displaying Alarm Configurations on page 180.
5. To check the status of active alarms, see “Checking Active Alarms” on page 178.

Table 92: Configuring Interface Alarms

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Alarm** level in the configuration hierarchy.	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.	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 an Ethernet link.	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: ■ 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	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**.	1. Enter set serial cts–absent yellow 2. Enter set serial dcd–absent yellow 3. Enter set serial loss–of–rx–clock red 4. Enter set serial loss–of–tx–clock red
Configure the system to generate the following interface alarms on a T3 link: ■ Red alarm when the remote endpoint is experiencing a Red failure ■ Yellow alarm when the upstream bit stream has more consecutive zeros than are permitted ■ Red alarm when there is a loss of signal on the interface	1. In the T3 field, click **Configure**. 2. From the Ylw list, select **red**. 3. From the Exz list, select **yellow**. 4. From the Los list, select **red**. 5. Click **OK**.	1. Enter set t3 ylw red 2. Enter set t3 exz yellow 3. Enter set t3 los red

Table 92: Configuring Interface Alarms *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the system to display active system alarms whenever a user with the login class admin logs in to the router. To define login classes, see the *JUNOS System Basics Configuration Guide*.	1. On the main Configuration page next to System, click **Configure** or **Edit**. 2. Next to Login, click **Configure** or **Edit**. 3. In the Class field, click **Add new entry**. 4. In the Class name field, type admin. 5. Select the **Login alarms** check box. 6. Click **OK**.	1. Enter edit system login 2. Enter set class admin login-alarms

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 taskbar appears in red. After you view the alarms, *Alarms* returns to white. If new alarms become active, *Alarms* is red until you again display the View Alarms page.

Figure 13 on page 179 shows the View Alarms summary page. Click an alarm in the list of active alarms to display a detailed alarm message.

Figure 13: J-Web View Alarms Summary Page

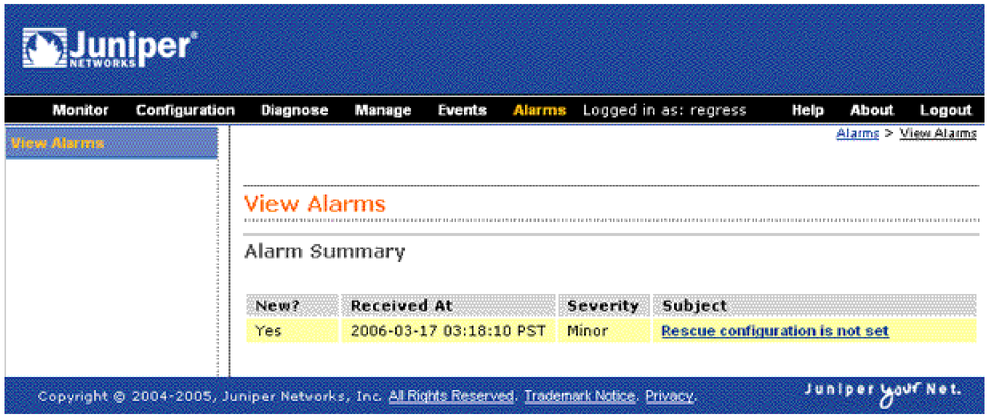


Table 93 on page 179 summarizes the output fields on the alarms page.

Table 93: 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.	
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.

Table 93: Summary of Key Alarm Output Fields *(continued)*

Field	Values	Additional Information
Alarm Type	Category of the alarm: ■ 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 an 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 show chassis alarms command.

```
[edit]
user@host# show chassis alarms
t3 {
   exz yellow;
   los red;
   ylw red;
}
ds1 {
   ylw red;
}
ethernet {
   link-down red;
}
serial {
   loss-of-rx-clock red;
   loss-of-tx-clock red;
   dcd-absent yellow;
   cts-absent yellow;
}
```

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
- Ethernet alarms
- Serial alarms

Related Topics 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

Chapter 10

Performing Software Upgrades and Reboots

A J-series Services Router is delivered with the JUNOS 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 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

Typically, you upgrade the JUNOS 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 Software 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.

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 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 192.

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 94 on page 187.

Table 94: Secondary Storage Devices for Backup

Storage Device	Available on Routers	Minimum Storage Required
External compact flash	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 193. For instructions about how to backup your system using the CLI, see "Configuring a Boot Device for Backup with the CLI" on page 196.

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 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 186.
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

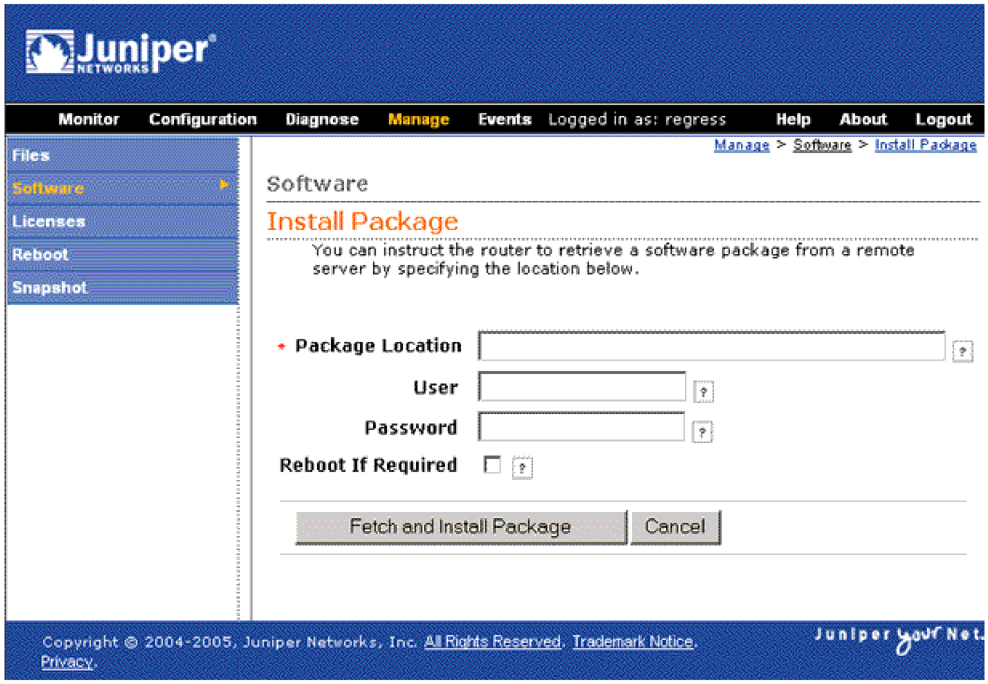
You can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the file to the router. This section contains the following topics:

Installing Software Upgrades from a Remote Server

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 14 on page 189 shows the Install Remote page for the router.

Figure 14: Install Remote Page



To install software upgrades from a remote server:

1. Download the software package as described in “Downloading Software Upgrades from Juniper Networks” on page 188.
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 95 on page 189.
4. Click **Fetch and Install Package**. The software is activated after the router has rebooted.

Table 95: 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: ftp://*hostname*/*pathname*/*package-name* http://*hostname*/*pathname*/*package-name*
User	Specifies the username, if the server requires one.	Type the username.

Table 95: Install Remote Summary *(continued)*

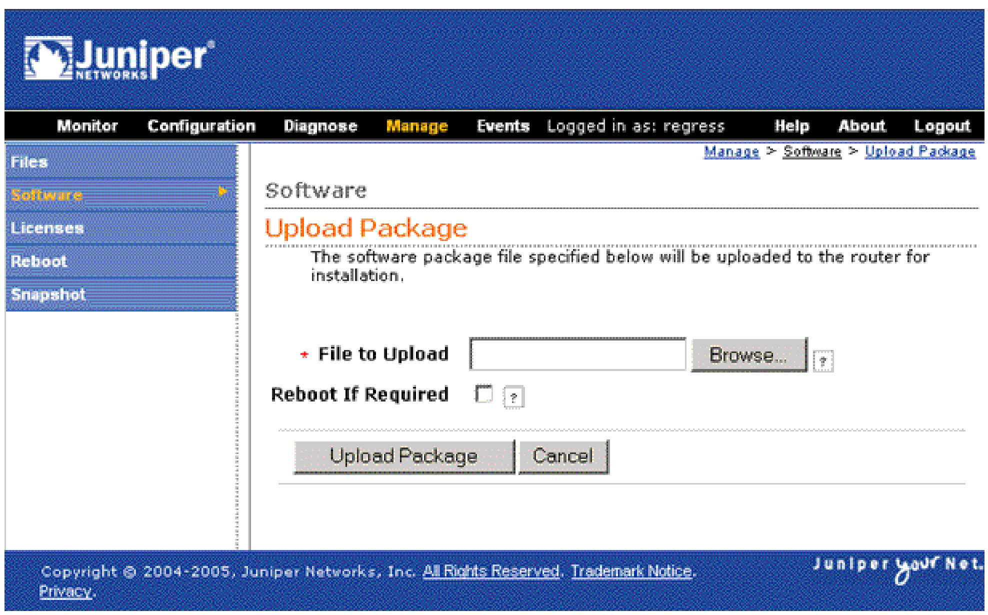
Field	Function	Your Action
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to reboot automatically when the upgrade is complete.

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 15 on page 190 shows the Upload Package page for the router.

Figure 15: 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 188.
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 96 on page 191.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 96: 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 188.
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 192
- Downgrading the Software with the CLI on page 192

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.

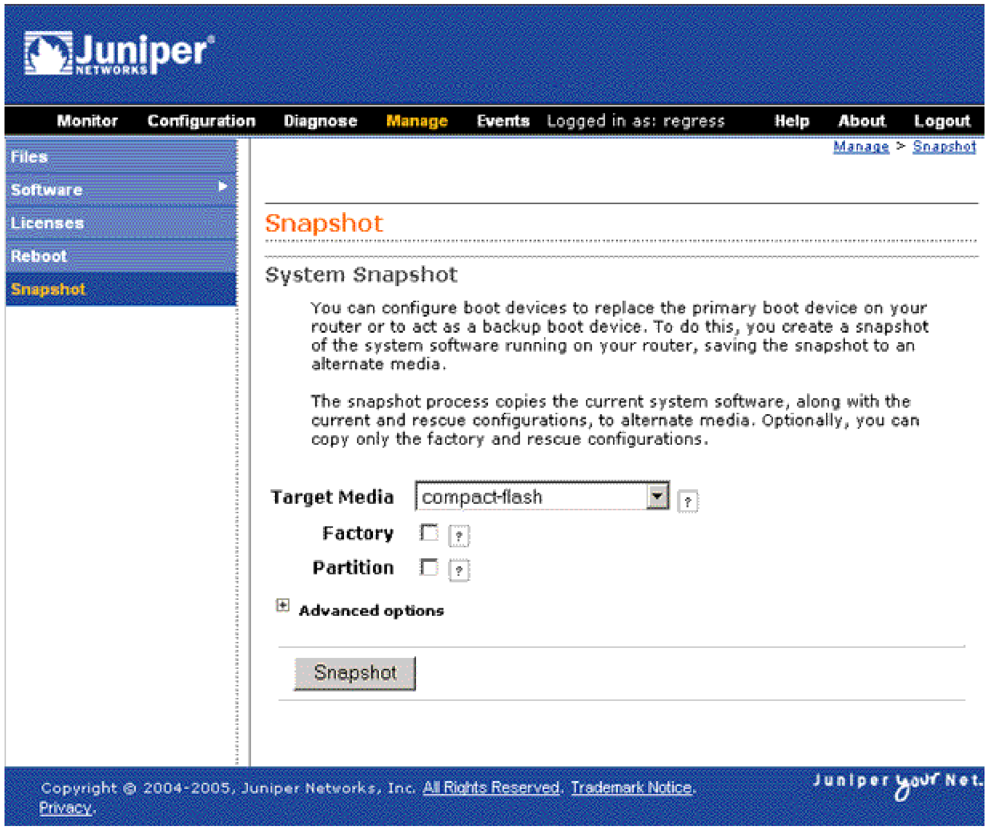
This section contains the following topics:

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

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 16 on page 194 shows the Snapshot page.

Figure 16: Snapshot Page



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 97 on page 194.
3. Click **Snapshot**.
4. Click **OK**.

Table 97: Snapshot Summary

Field	Function	Your Action
Target Media	Specifies the boot device to copy the snapshot to. **NOTE:** You cannot copy software to the active boot device.	In the list, select a boot device that is not the active boot device: ■ **compact-flash**—Copies software to the internal compact flash. ■ **removable-compact-flash**—Copies software to the external compact flash. This option is available on J4300 and J6300 Services Routers only. ■ **usb**—Copies software to the device connected to the USB port.

Table 97: Snapshot Summary *(continued)*

Field	Function	Your Action
Factory	Copies only default files that were loaded on the internal compact flash when it was shipped from the factory, plus the rescue configuration, if one has been set. **NOTE:** After a boot device is created with the default factory configuration, it can operate only in an internal compact flash slot.	To copy only the default factory configuration, plus a rescue configuration if one exists, select the check box.
Partition	Partitions the medium. This process is usually necessary for boot devices that do not already have software installed on them.	To partition the medium that you are copying the snapshot to, select the check box.
As Primary Media	On an external compact flash or USB storage device only, creates a snapshot for use as the primary boot medium. Use this feature to replace the medium in the internal compact flash slot or to replicate it for use in another Services Router. This process also partitions the boot medium. **NOTE:** After the boot device is created as an internal compact flash, it can operate only in an internal compact flash slot.	To create a boot medium to use in the internal compact flash only, select the check box.
Data Size	Specifies the size of the data partition, in kilobytes. The data partition is mounted on /data. This space is not used by the router, and can be used for extra storage. This selection also partitions the boot medium.	Type a numeric value, in kilobytes. The default value is 0 KB.
Swap Size	Specifies the size of the swap partition, in kilobytes. 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 197. This selection also partitions the boot medium.	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.

Table 97: Snapshot Summary *(continued)*

Field	Function	Your Action
Config Size	Specifies the size of the config partition, in kilobytes. The config partition is mounted on /config. The configuration files are stored in this partition. This selection also partitions the boot medium.	Type a numeric value, in kilobytes. The default value is 10 percent of physical memory on the boot medium.
Root Size	Specifies the size of the root partition, in kilobytes. The root partition is mounted on / and does not include configuration files. This selection also partitions the boot medium.	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 98 on page 196 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 98: CLI request system snapshot Command Options

Option	Description
as-primary	On an external compact flash or USB storage device only, creates a snapshot for use as the primary boot medium. Use the as-primary option to replace the medium in the internal compact flash slot or to replicate it for use in another Services Router. This process also partitions the boot medium. **NOTE:** After the boot device is created as an internal compact flash, it can operate only in an internal compact flash slot.
config-size *size*	Specifies the size of the config partition, in megabytes. The default value is 10 percent of physical memory on the boot medium. The config partition is mounted on /config. The configuration files are stored in this partition. This option also partitions the boot medium.

Table 98: CLI request system snapshot Command Options *(continued)*

Option	Description
data-size *size*	Specifies the size of the data partition, in megabytes. The default value is 0 MB. The data partition is mounted on /data. This space is not used by the router, and can be used for extra storage. This option also partitions the boot medium.
factory	Copies only default files that were loaded on the internal compact flash when it was shipped from the factory, plus the rescue configuration if one has been set. **NOTE:** After the boot medium is created with the factory option, it can operate in only the internal compact flash slot.
media *type*	Specifies the boot device the software snapshot is copied to: ■ compact-flash—Copies software to the internal compact flash. ■ removable-compact-flash—Copies software to the external compact flash. This option is available on J4300 and J6300 Services Routers only. ■ usb—Copies software to the device connected to the USB port. **NOTE:** You cannot copy software to the active boot device.
partition	Partitions the medium. This option is usually necessary for boot devices that do not have software already installed on them.
root-size *size*	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. The root partition is mounted on / and does not include configuration files. This option also partitions the boot medium.
swap-size *size*	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. 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 197. **NOTE:** This option also partitions the boot medium.

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 99 on page 198 describes the set system dump-device command options.

Table 99: CLI set system dump-device Command Options

Option	Description
boot-device	Uses whatever device was booted from as the system software failure memory snapshot device.
compact-flash	Uses the internal compact flash as the system software failure memory snapshot device.
removable-compact-flash	Uses the compact flash 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 to store the JUNOS software, router configuration files, and log files. The internal compact flash 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 internal compact flash, J4300 and J6300 Services Routers have a slot in the front of the chassis for external 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 199
- Recommended Recovery Hardware and Software on page 199
- Configuring Internal Compact Flash Recovery on page 200

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 192.)

If the internal compact flash fails at startup, the Services Router automatically boots itself from the external 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 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 internal compact flash is lost.

Recommended Recovery Hardware and Software

Before configuring compact flash recovery, assemble the equipment and software listed in Table 100 on page 199.

Table 100: 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
Adapter appropriate for your system	■ 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: ■ 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	■ UNIX with PCMCIA drivers ■ Windows 2000, or Windows XP

Table 100: Recommended Recovery Hardware and Software *(continued)*

Recommended Hardware and Software	Examples

Systems running Windows require additional software.	■ WinZip, gzip, or a similar compression utility
	■ A utility such as the following that allows you to write files to unformatted devices:
	  ■ Norton Ghost
	  ■ dd utility from the Cygwin package
	  ■ physdiskwrite utility

Configuring Internal Compact Flash Recovery

To recover an internal compact flash with a corrupt or missing operating system, you must remove the corrupt internal compact from the J-series Services Router, plug it into a PC with a PCMIA 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 an internal compact flash, 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 188.)

To recover an internal compact flash:

1. Plug the compact flash 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. 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 186.
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 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 in250368+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, you can use it as the internal compact flash in any J-series Services Router. For installation instructions, see the Getting Started Guide for your router.

Rebooting or Halting a Services Router

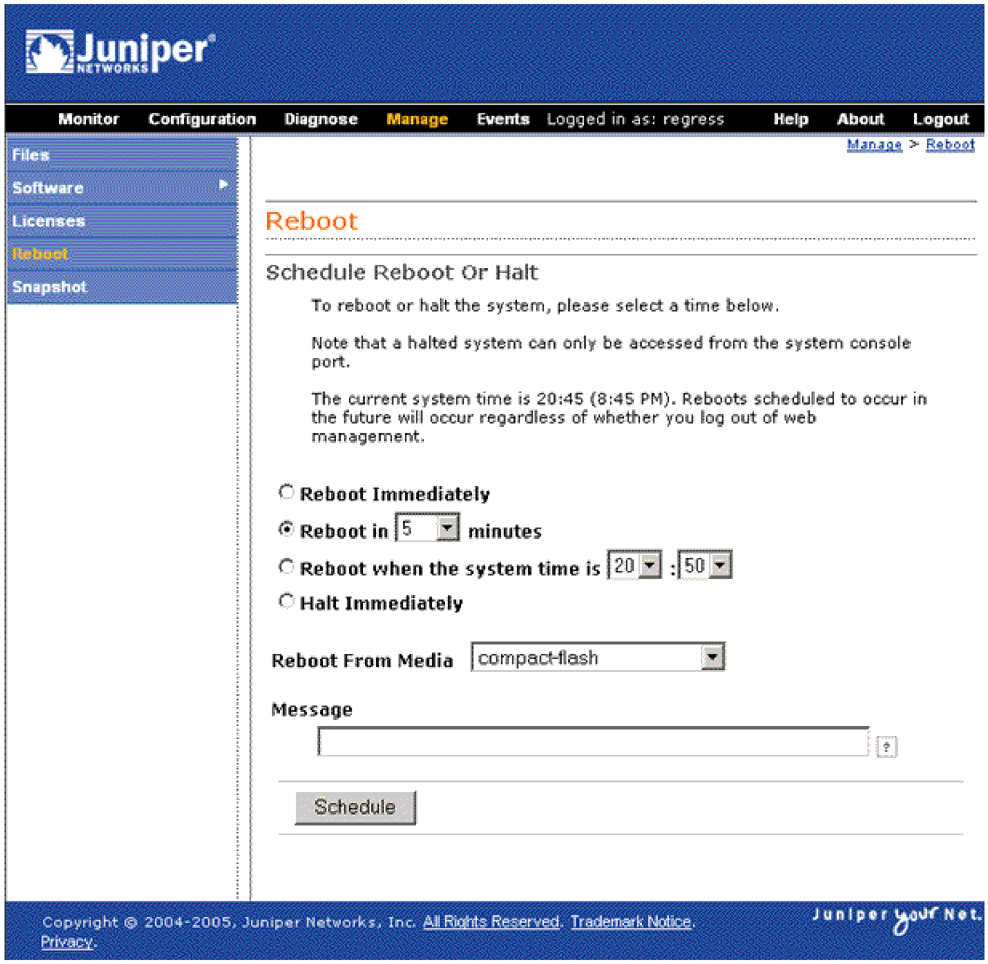
Reboot or halt a Services Router with either the J-Web interface or the CLI. This section contains the following topics:

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

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

Figure 17 on page 202 shows the Reboot page for the router.

Figure 17: Reboot Page



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 internal compact flash. This selection is the default choice.
   - **removable-compact-flash**—Reboots from the optional external compact flash. 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 101 on page 203 describes the request system reboot command options.

Table 101: CLI Request System Reboot Command Options

Option	Description
none	Same as at now (reboots the router immediately).

Table 101: CLI Request System Reboot Command Options *(continued)*

Option	Description
at *time*	Specifies the time at which to reboot the router. You can specify time in one of the following ways: ■ now—Reboots the router immediately. This is the default. ■ +*minutes*—Reboots the router in the number of minutes from now that you specify. ■ *yymmddhhmm*—Reboots the router at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute. ■ *hh:mm*—Reboots the 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.
in *minutes*	Specifies the number of minutes from now to reboot the router. This option is a synonym for the at +*minutes* option.
media *type*	Specifies the boot device to boot the router from: ■ compact-flash—Reboots from the internal compact flash. This is the default. ■ removable-compact-flash—Reboots from the optional external compact flash. This option is available on J4300 and J6300 Services Routers only. ■ usb—Reboots from the USB storage device.
message *"text"*	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 102 on page 204 describes the request system halt command options.

Table 102: CLI Request System Halt Command Options

Option	Description
none	Same as at now (stops software processes on the router immediately).

Table 102: CLI Request System Halt Command Options *(continued)*

Option	Description
at *time*	Time at which to stop the software processes on the router. You can specify time in one of the following ways: ■ now—Stops the software processes immediately. This is the default. ■ *+minutes*—Stops the software processes in the number of minutes from now that you specify. ■ *yymmddhhmm*—Stops the software processes at the absolute time you specify. Enter the year, month, day, hour (in 24-hour format), and minute. ■ *hh:mm*—Stops the software processes at the absolute time that you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
in *minutes*	Specifies the number of minutes from now to stop the software processes on the router. This option is a synonym for the at *+minutes* option.
media *type*	Specifies the boot device to boot the router from after the halt: ■ compact-flash—Reboots from the internal compact flash. This is the default. ■ removable-compact-flash—Reboots from the optional external compact flash. This option is available on J4300 and J6300 Services Routers only. ■ usb—Reboots from the USB storage device.
message *"text"*	Provides a message to display to all system users before the software processes on the router are stopped.

Chapter 11
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

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

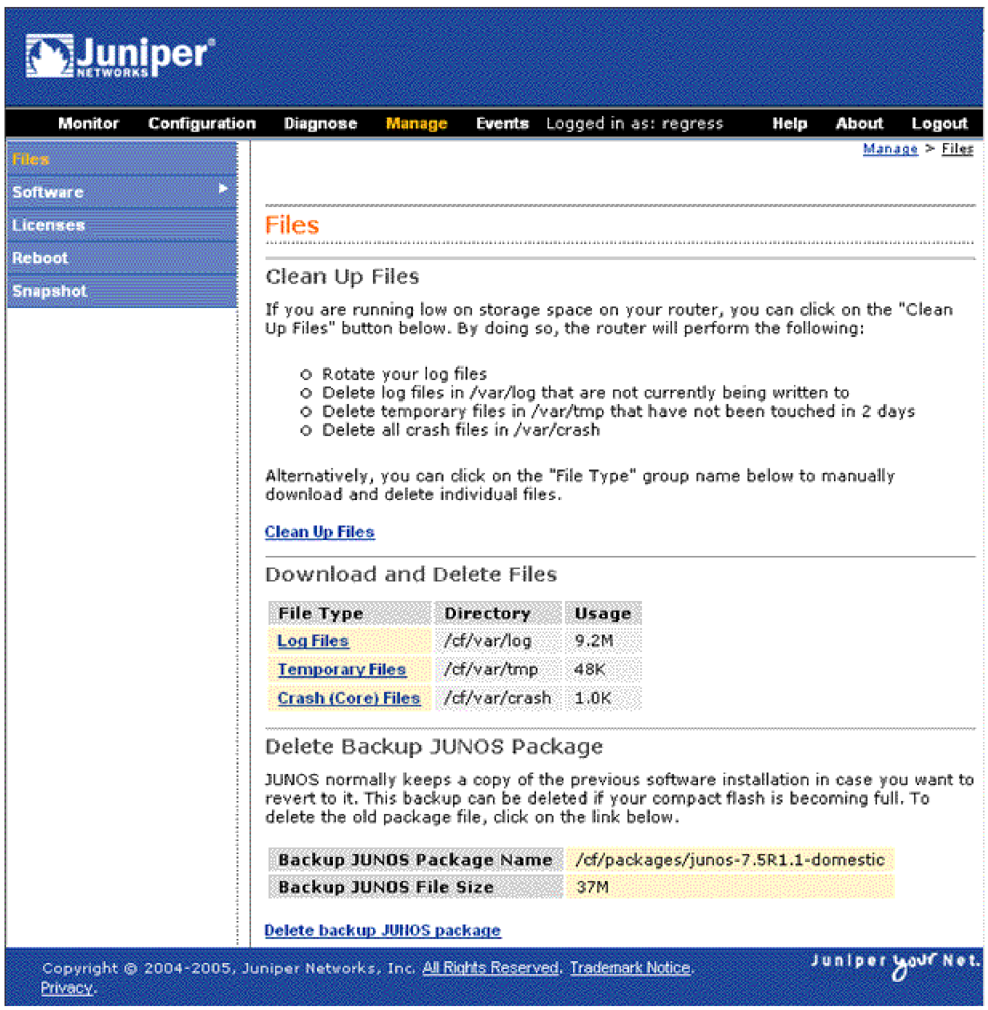
You can use the J-Web interface to rotate log files and delete unnecessary files on the Services Router. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.

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 18 on page 208 shows the Clean Up Files page.

Figure 18: Clean Up Files Page



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

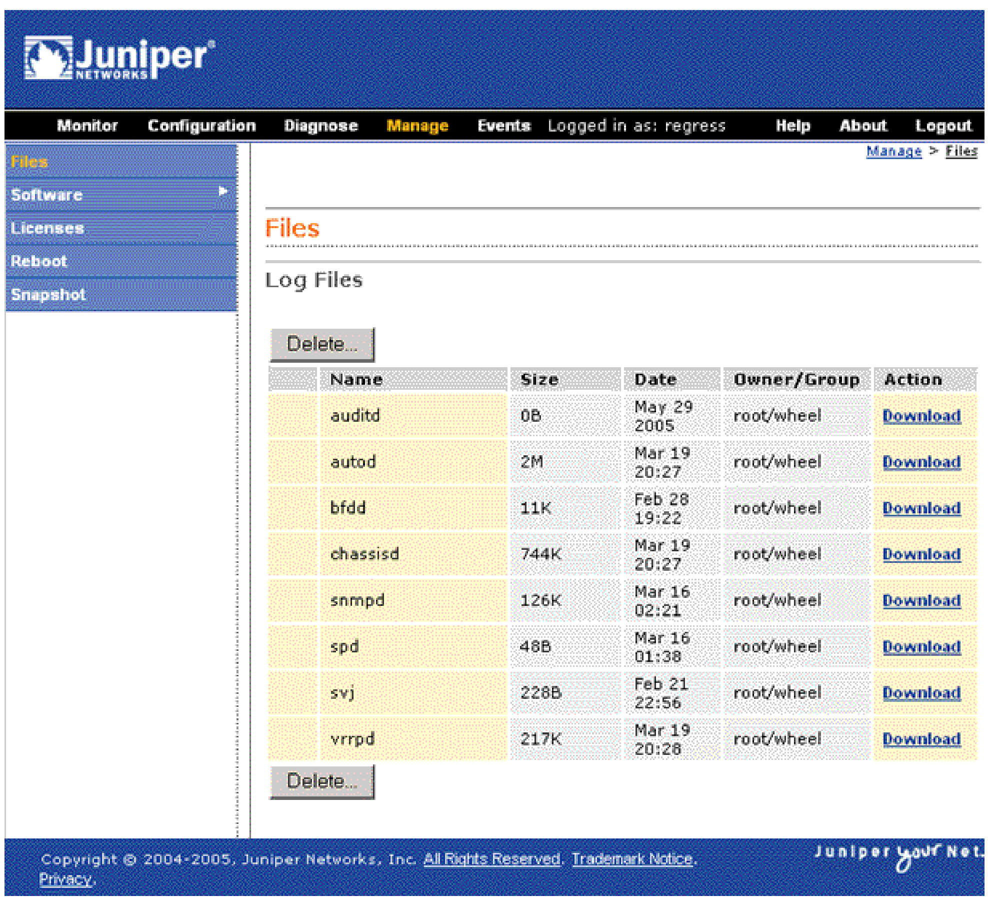
1. In the J-Web interface, select **Manage > Files**.
2. In the Clean Up Files section, click **Clean Up Files**. The router rotates log files and identifies the files that can be safely deleted.
3. The J-Web interface displays the files that you can delete and the amount of space that will be freed 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 19 on page 209 shows the J-Web page from which you can download log files.

Figure 19: Log Files Page (Download)



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.

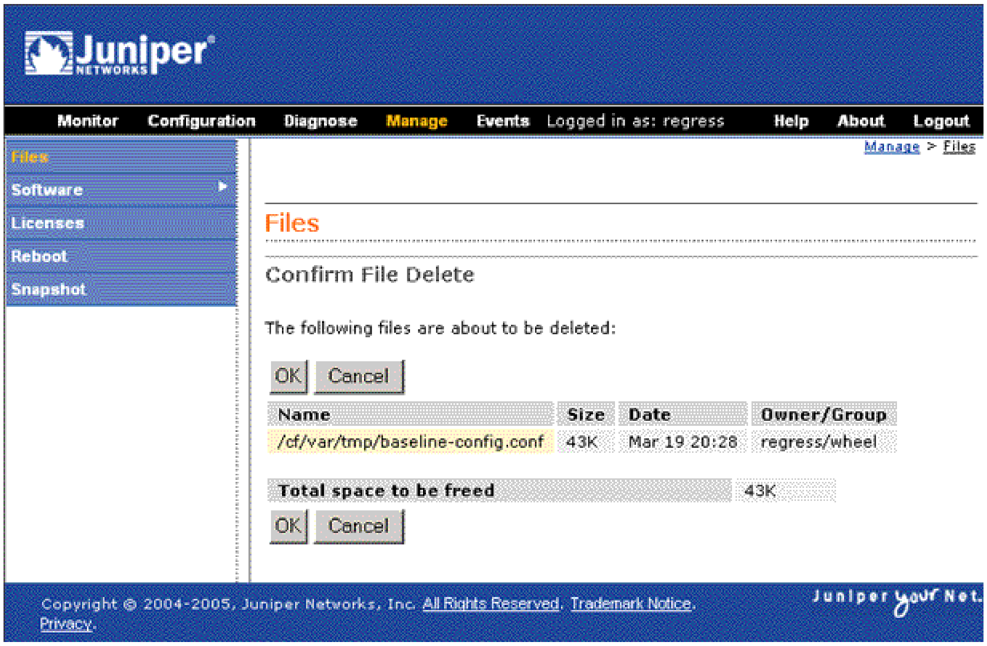
Deleting Files

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 207. This tool determines which files can be safely deleted from the file system.

Figure 20 on page 211 shows the J-Web page on which you confirm the deletion of files.

Figure 20: 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.

Managing Accounting Files

If you configure your system to capture accounting data in log files, set the location for accounting files to the DRAM.

The default location for accounting files is the cfs/var/log directory on the compact flash. The nonpersistent option minimizes the read/write traffic to your compact flash. We recommend that you use the nonpersistent option for all accounting files configured on your system.

To store accounting log files in DRAM instead of the compact flash:

1. Enter the configuration mode in the CLI.

2. To create an accounting data log file in DRAM, enter the following command, replacing *filename* with the name of the file:

```
user@host> edit accounting-options file filename
```

3. To store accounting log files in the DRAM file, enter the following command:

```
user@host> set file filename nonpersistent
```

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

CAUTION: If log files for accounting data are stored on DRAM, these files are lost when the router reboots. Therefore, we recommend that you back up these files periodically.

Encrypting and Decrypting Configuration Files

Configuration files contain sensitive information such as IP addresses. By default, the Services Router stores configuration files in unencrypted format on an external compact flash. This storage method is considered a security risk because the compact flash 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 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 214
- Decrypting Configuration Files on page 215
- Modifying the Encryption Key on page 215

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 103 on page 214.

Table 103: 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: ■ 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:juniper1

Verifying EEPROM stored encryption key:
```

4. At the second prompt, reenter the encryption key.
5. Enter configuration mode in the CLI.

6. To enable configuration file encryption to take place, enter the following commands:

```
user@host# edit system

user@host# set encrypt-configuration-files
```

7. To begin the encryption process, commit the configuration.

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

Decrypting Configuration Files

To disable the encryption of configuration files on a 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 103 on page 214. For example:

```
user@host> request system set-encryption-key

Enter EEPROM stored encryption key:
```

3. At the prompt, enter the new encryption key. The encryption key must have at least 6 characters.

```
Enter EEPROM stored encryption key:juniperone

Verifying EEPROM stored encryption key:
```

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

Part 4

Diagnosing Performance and Network Problems

Chapter 12

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

Before diagnosing J-series Services Routers, become familiar with the terms defined in Table 104 on page 219.

Table 104: 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 104: 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 107.

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 105 on page 220 describes the functions of the Diagnose and Manage options.

Table 105: 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 226.

Table 105: 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 223.
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 235.
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 239.
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 207.
Upgrade	Allows you to upgrade and manage Services Router software packages. For details, see "Performing Software Upgrades and Reboots" on page 185.
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 201.

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 106 on page 222.

Table 106: CLI Diagnostic Command Summary

Command	Function
Controlling the CLI Environment	
set *option*	Configures the CLI display.
Diagnosis and Troubleshooting	
clear	Clears statistics and protocol database information.
mtrace	Traces information about multicast paths from source to receiver. For details, see "Tracing Multicast Routes from the CLI" on page 254.
monitor	Performs real-time debugging of various software components, including the routing protocols and interfaces. For details, see the following sections: ■ Using the monitor interface Command on page 259 ■ Using the monitor traffic Command on page 260 ■ Displaying Log and Trace Files from the CLI on page 258
ping	Determines the reachability of a remote network host. For details, see "Pinging Hosts from the CLI" on page 244.
ping mpls	Determines the reachability of an MPLS endpoint using various options. For details, see "MPLS Connection Checking" on page 223.
test	Tests the configuration and application of policy filters and AS path regular expressions.
traceroute	Traces the route to a remote network host. For details, see "Tracing Unicast Routes from the CLI" on page 251.
Connecting to Other Network Systems	
ssh	Opens secure shell connections. For details, see "Using the ssh Command" on page 28.
telnet	Opens Telnet sessions to other hosts on the network. For details, see "Using the telnet Command" on page 27.
Management	
copy	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.
restart *option*	Restarts the various JUNOS software processes, including the routing protocol, interface, and SNMP processes.
request	Performs system-level operations, including stopping and rebooting the Services Router and loading JUNOS software images.

Table 106: CLI Diagnostic Command Summary *(continued)*

Command	Function
start	Exits the CLI and starts a UNIX shell.
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 107 on page 223 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 107: Options for Checking MPLS Connections

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping RSVP-signaled LSP	ping mpls rsvp	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The 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.

Table 107: Options for Checking MPLS Connections *(continued)*

J-Web Ping MPLS Tool	ping mpls Command	Purpose	Additional Information
Ping LDP-signaled LSP	ping mpls ldp	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The 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.
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.	For information about interface names, See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.
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

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 13 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

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 244.)

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 21 on page 227).
3. Enter information into the Ping Host page, as described in Table 108 on page 227.

   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 22 on page 229). 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 109 on page 229 summarizes the output fields of the display.
5. To stop the ping operation before it is complete, click **OK**.

Figure 21: Ping Host Page

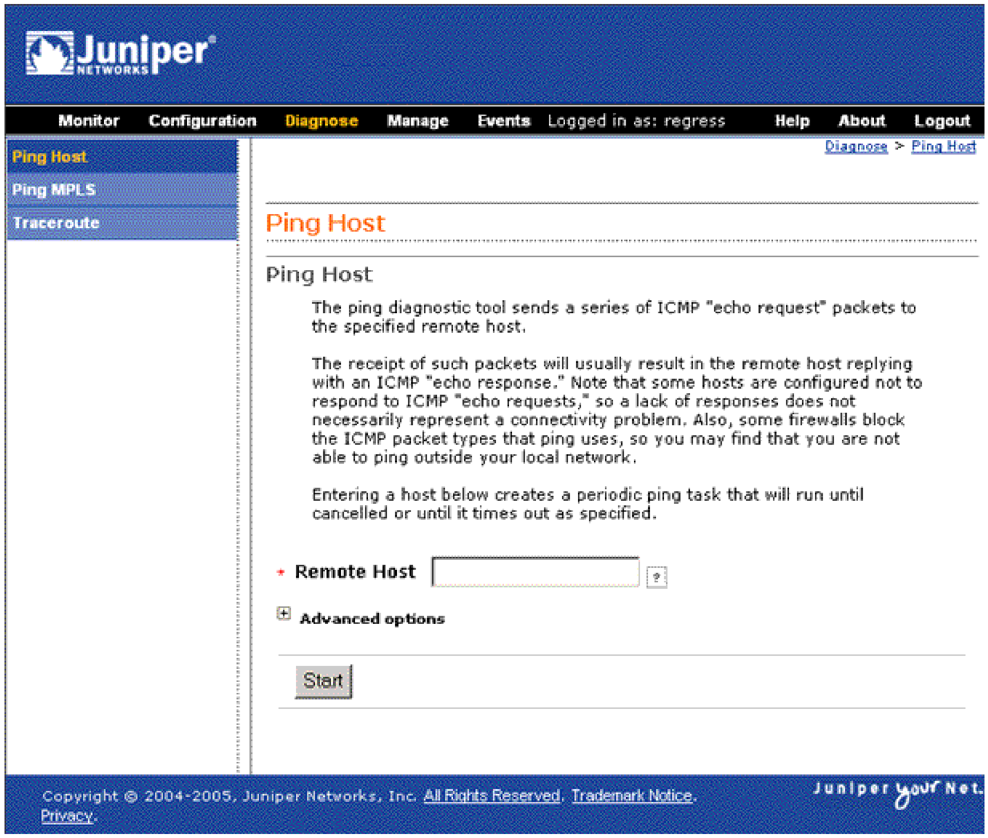


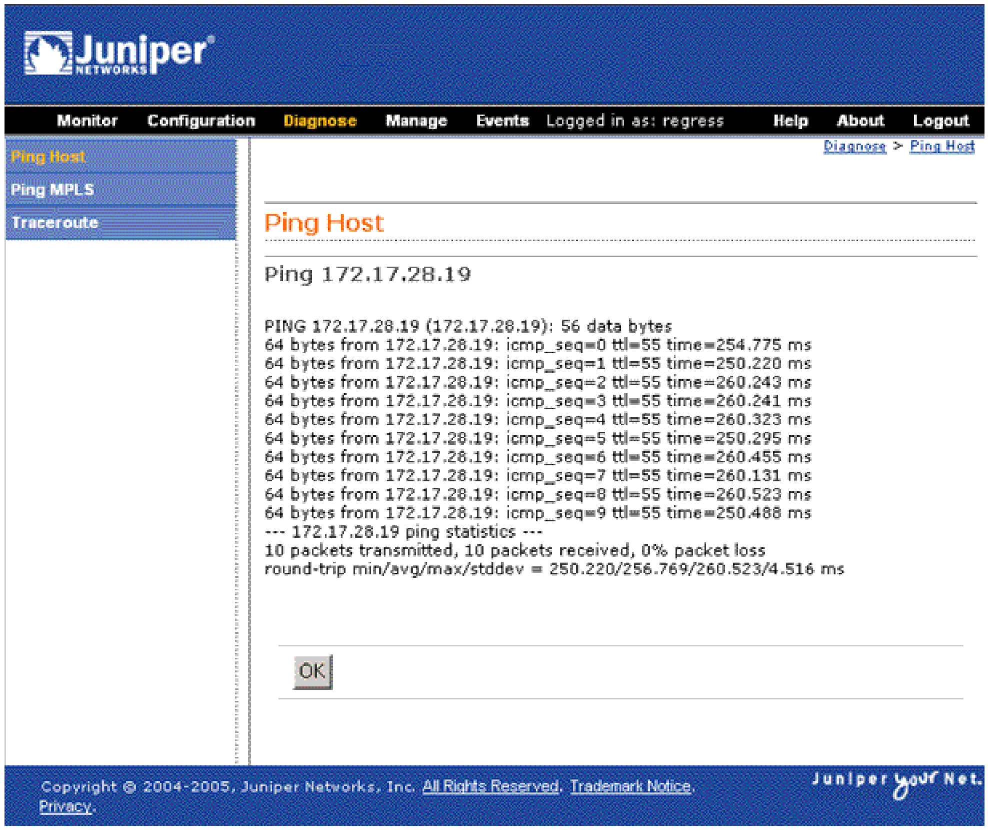
Table 108: J-Web Ping Host Field Summary

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.	■ To suppress the display of the hop hostnames, select the check box. ■ To display the hop hostnames, clear the check box.
Interface	Specifies the interface on which the ping requests are sent.	From the list, select the interface on which ping requests are sent. If you select **any**, the ping requests are sent on all interfaces.
Count	Specifies the number of ping requests to send.	From the list, select the number of ping requests to send.
Don't Fragment	Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet.	■ To set the DF bit, select the check box. ■ To clear the DF bit, clear the check box.

Table 108: J-Web Ping Host Field Summary *(continued)*

Field	Function	Your Action
Record Route	Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane.	■ 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	Determines whether ping requests are routed by means of the routing table. 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.	■ 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 22: Ping Host Results Page



Ping Host Results and Output Summary

Table 109 on page 229 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 109 on page 229 for a possible explanation.

Table 109: J-Web Ping Host Results and Output Summary

Ping Host Result	Description
bytes bytes from *ip-address*	■ *bytes*—Size of ping response packet, which is equal to the value you entered in the Packet Size box, plus 8. ■ *ip-address*—IP address of destination host that sent the ping response packet.
icmp_seq=0 icmp_seq=*number*	*number*—Sequence Number field of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
ttl=*number*	*number*—Time-to-live hop-count value of the ping response packet.
time=*time*	*time*—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.

Table 109: J-Web Ping Host Results and Output Summary *(continued)*

Ping Host Result	Description
number packets transmitted	*number*—Number of ping requests (probes) sent to host.
number packets received	*number*—Number of ping responses received from host.
percentage packet loss	*percentage*—Number of ping responses divided by the number of ping requests, specified as a percentage.
round-trip min/avg/max/stddev = *min-time/avg-time/max-time/std-dev* ms	■ *min-time*—Minimum round-trip time (see time=*time* field in this table). ■ *avg-time*—Average round-trip time. ■ *max-time*—Maximum round-trip time. ■ *std-dev*—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 244.

Before using the J-Web ping MPLS tool in your network, read “Ping MPLS Preparation” on page 225.

This section contains the following topics:

- Using the J-Web Ping MPLS Tool on page 231
- Ping MPLS Results and Output on page 234

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 23 on page 232).
3. Enter information into the Ping MPLS page, as described in Table 110 on page 232.
4. Click **Start**.

   Table 111 on page 235 summarizes the output fields of the display.
5. To stop the ping operation before it is complete, click **OK**.

Figure 23: Ping MPLS Page

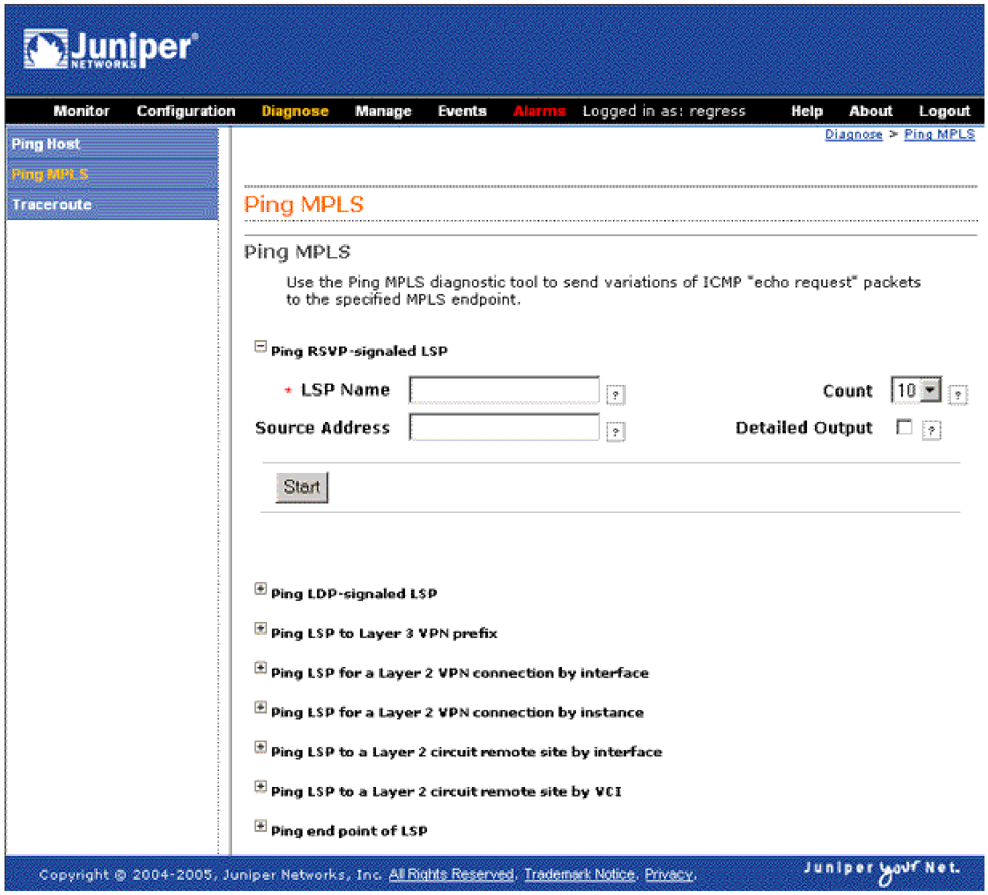


Table 110: J-Web Ping MPLS Field Summary

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.
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.

Table 110: J-Web Ping MPLS 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. 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. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	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 110: 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 111 on page 235 summarizes the output in the ping MPLS display. If the Services Router receives no responses from the destination host, review the list after Table 111 on page 235 for a possible explanation.

Table 111: 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.
number packets transmitted	*number*—Number of ping requests (probes) sent to a host.
number packets received	*number*—Number of ping responses received from a host.
percentage packet loss	*percentage*—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 236
- Traceroute Results and Output Summary on page 238

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 24 on page 237).
3. Enter information into the Traceroute page, as described in Table 112 on page 237.

   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 113 on page 238 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 24: Traceroute Page

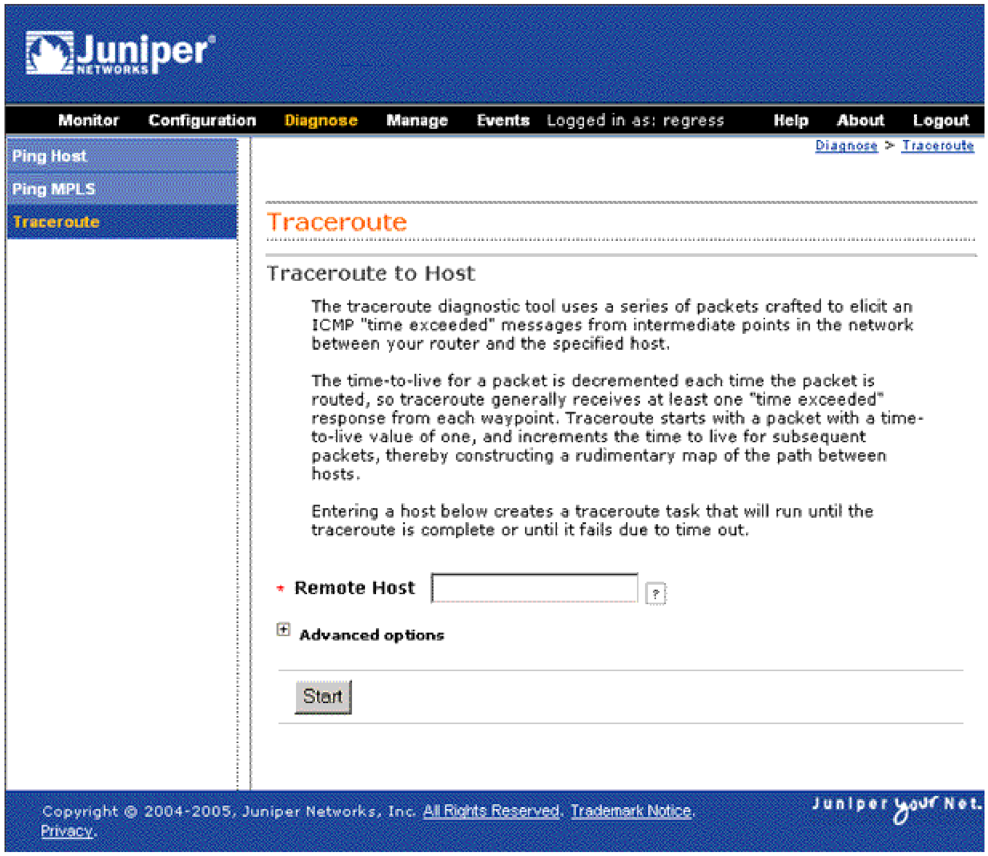


Table 112: Traceroute Field Summary

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.	■ To suppress the display of the hop hostnames, select the check box. ■ To display the hop hostnames, clear the check box.
Gateway	Specifies the IP address of the gateway to route through.	Type the gateway IP address.
Source Address	Specifies the source address of the outgoing traceroute packets.	Type the source IP address.

Table 112: Traceroute Field Summary *(continued)*

Field	Function	Your Action
Bypass Routing	Determines whether traceroute packets are routed by means of the routing table. 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.	■ 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.	■ 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 113 on page 238 summarizes the output in the traceroute display. If the Services Router receives no responses from the destination host, review the list after Table 113 on page 238 for a possible explanation.

Table 113: J-Web Traceroute Results and Output Summary

Field	Description
hop-number	Number of the hop (router) along the path.
host	Hostname, if available, or IP address of the router. If the Don't Resolve Addresses check box is selected, the hostname is not displayed.
ip-address	IP address of the router.
as-number	AS number of the router.
time1	Round-trip time between the sending of the first traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.
time2	Round-trip time between the sending of the second traceroute packet and the receiving of the corresponding Time Exceeded packet from that particular router.
time3	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 260.

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 267.

This section contains the following topics:

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 25 on page 240) as described in Table 114 on page 241.

The sample configuration in Table 114 on page 241 captures the next 10 TCP packets originating from the IP address 10.1.40.48 on port 23 and passing through the Gigabit Ethernet interface ge-0/0/0.

3. To save the captured packets to a file, or specify other advanced options, click the expand icon next to Advanced options, and enter information as described in Table 114 on page 241.

4. Click **Start**.

   The captured packet headers are decoded and displayed in the Packet Capture display (see Figure 26 on page 243).

   Table 115 on page 243 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 25: Packet Capture Page

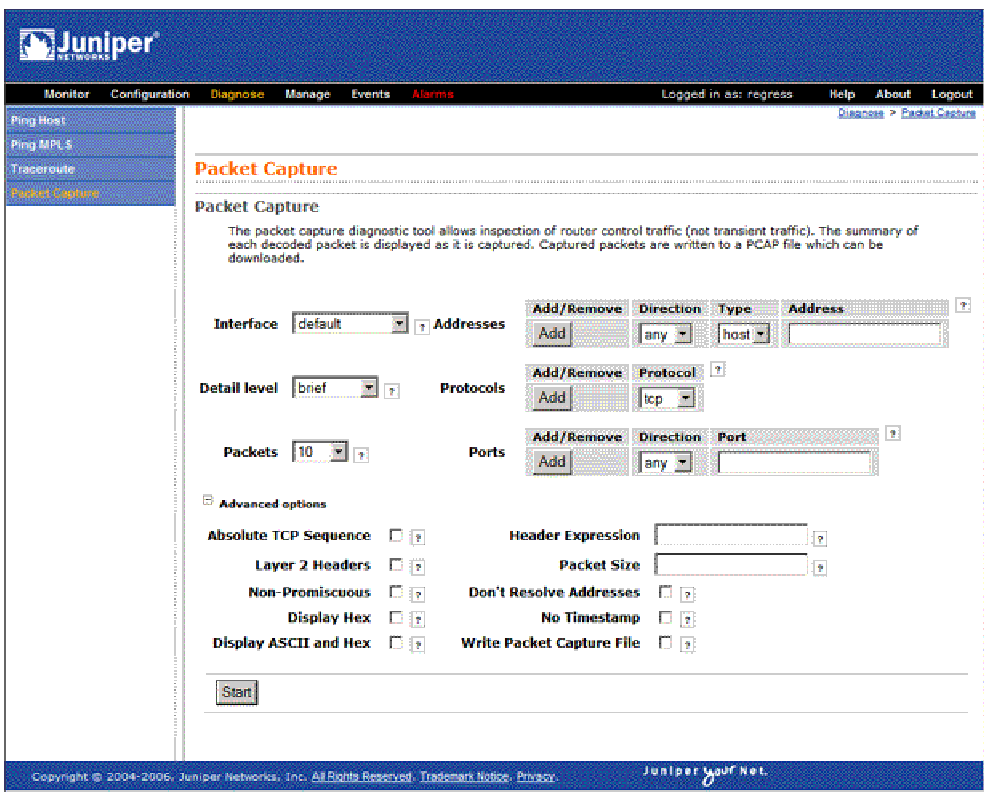


Table 114: Packet Capture Field Summary

Field	Function	Your Action
Interface	Specifies the interface on which the packets are captured. If you select **default**, packets on the Ethernet management port 0, are captured.	From the list, select an interface—for example, ge-0/0/0.
Detail level	Specifies the extent of details to be displayed for the packet headers. ■ 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	Specifies the addresses to be matched for capturing the packets using a combination of the following parameters: ■ 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. You can add multiple entries to refine the match criteria for addresses.	Select address-matching criteria. For example: 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.	Select a direction and a port. For example: 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.	■ 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.

Table 114: Packet Capture Field Summary *(continued)*

Field	Function	Your Action
Layer 2 Headers	Specifies that link-layer packet headers are to be displayed.	■ To include link-layer packet headers while capturing packets, select this check box. ■ To exclude link-layer packet headers while capturing packets, clear this check box.
Non-Promiscuous	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.	■ 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.	■ 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.	■ 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.	■ 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.	■ 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 /var/tmp. The files are named with the prefix jweb-pcap and the extension .pcap. If you select this option, the decoded packet headers are not displayed on the packet capture page.	■ 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 26 on page 243 shows J-Web packet capture output from router1, with the level of detail set to brief. Table 115 on page 243 summarizes the output in the packet capture display.

Figure 26: Packet Capture Results Page

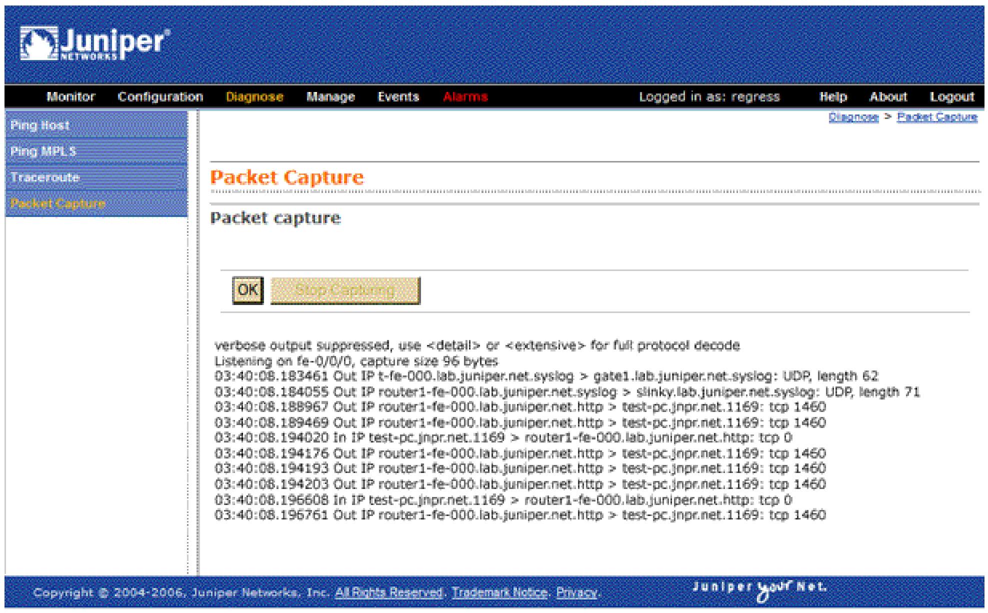


Table 115: J-Web Packet Capture Results and Output Summary

Field	Description
timestamp	Time when the packet was captured. The timestamp 00:45:40.823971 means 00 hours (12.00 a.m.), 45 minutes, and 40.823971 seconds. **NOTE:** The time displayed is local time.
direction	Direction of the packet. Specifies whether the packet originated from the Routing Engine (Out), or was destined for the Routing Engine (In).
protocol	Protocol for the packet. In the sample output, IP indicates the Layer 3 protocol.
source address	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 115: J-Web Packet Capture Results and Output Summary *(continued)*

Field	Description
destination address	Hostname, if available, or IP address of the packet's destination with the port number. If the Don't Resolve Addresses check box is selected, only the IP address of the destination and the port are displayed. **NOTE:** When a string is defined for the port, the packet capture output displays the string instead of the port number.
protocol	Protocol for the packet. In the sample output, TCP indicates the Layer 4 protocol.
data size	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 221.

This section contains the following topics:

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 226.)

Enter the ping command with the following syntax. Table 116 on page 245 describes the ping command options.

```
user@host> ping host <interface source-interface> <bypass-routing> <count number>
<do-not-fragment> <inet | inet6> <interval seconds> <loose-source [hosts]>
<no-resolve> <pattern string> <rapid> <record-route>
<routing-instance routing-instance-name> <size bytes> <source source-address>
```

<strict> **<strict-source** [*hosts*]**>** **<tos** *number***>** **<ttl** *number***>** **<wait** *seconds***>** **<detail>** **<verbose>**

To quit the ping command, press Ctrl-C.

Table 116: CLI ping Command Options

Option	Description
host	Pings the hostname or IP address you specify.
interface *source-interface*	(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*number*	(Optional) Limits the number of ping requests to send. Specify a count from 1 through 2,000,000,000. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
do-not-fragment	(Optional) Sets the Don't Fragment (DF) bit in the IP header of the ping request packet.
inet	(Optional) Forces the ping requests to an IPv4 destination.
inet6	(Optional) Forces the ping requests to an IPv6 destination.
interval *seconds*	(Optional) Sets the interval between ping requests, in seconds. Specify an interval from 0.1 through 10,000. The default value is 1 second.
loose-source [*hosts*]	(Optional) For IPv4, sets the loose source routing option in the IP header of the ping request packet.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
pattern *string*	(Optional) Includes the hexadecimal string you specify, in the ping request packet.
rapid	(Optional) Sends ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the count option.
record-route	(Optional) For IPv4, sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed on the screen.
routing-instance *routing-instance-name*	(Optional) Uses the routing instance you specify for the ping request.
size *bytes*	(Optional) Sets the size of the ping request packet. Specify a size from 0 through 65,468. The default value is 56 bytes, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.
source *source-address*	(Optional) Uses the source address that you specify, in the ping request packet.
strict	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet.

Table 116: CLI ping Command Options *(continued)*

Option	Description
strict-source [*hosts*]	(Optional) For IPv4, sets the strict source routing option in the IP header of the ping request packet, and uses the list of hosts you specify for routing the packet.
tos *number*	(Optional) Sets the type-of-service (TOS) value in the IP header of the ping request packet. Specify a value from 0 through 255.
ttl *number*	(Optional) Sets the time-to-live (TTL) value for the ping request packet. Specify a value from 0 through 255.
wait *seconds*	(Optional) Sets the maximum time to wait after sending the last ping request packet. If you do not specify this option, the default delay is 10 seconds. If you use this option without the count option, the Services Router uses a default count of 5 packets.
detail	(Optional) Displays the interface on which the ping response was received.
verbose	(Optional) Displays detailed output.

Following is sample output from a ping command:

```
user@host> ping host3 count 4
PING host3.site.net (176.26.232.111): 56 data bytes
64 bytes from 176.26.232.111: icmp_seq=0 ttl=122 time=0.661 ms
64 bytes from 176.26.232.111: icmp_seq=1 ttl=122 time=0.619 ms
64 bytes from 176.26.232.111: icmp_seq=2 ttl=122 time=0.621 ms
64 bytes from 176.26.232.111: icmp_seq=3 ttl=122 time=0.634 ms

--- host3.site.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

The fields in the display are the same as those displayed by the J-Web ping host diagnostic tool. For information, see “Ping Host Results and Output Summary” on page 229.

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 230.

Before using ping mpls commands in your network, read “Ping MPLS Preparation” on page 225.

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 247
- Pinging Layer 3 VPNs on page 248
- Pinging Layer 2 VPNs on page 249
- Pinging Layer 2 Circuits on page 250

Pinging RSVP-Signaled LSPs and LDP-Signaled LSPs

Enter the ping mpls command with the following syntax. Table 117 on page 247 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 230.)

Table 117: CLI ping mpls ldp and ping mpls lsp-end-point Command Options

Option	Description
ldp *fec*	Pings an LDP-signaled LSP identified by the forwarding equivalence class (FEC) prefix and length.
lsp-end-point *prefix-name*	Pings an LSP endpoint using either an LDP FEC or a RSVP LSP endpoint address.
rsvp *lsp-name*	Pings an RSVP-signaled LSP identified by the specified LSP name.
exp *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(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 *source-address*	(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 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 234.

Pinging Layer 3 VPNs

Enter the ping mpls l3vpn command with the following syntax. Table 118 on page 248 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 230.)

Table 118: CLI ping mpls l3vpn Command Options

Option	Description
l3vpn prefix *prefix-name*	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.
l3vpn-name	(Optional) Layer 3 VPN name.
bottom-label-ttl	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
exp *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(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 *source-address*	(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 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 234.

Pinging Layer 2 VPNs

Enter the ping mpls l2vpn command with the following syntax. Table 119 on page 249 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 230.)

Table 119: CLI ping mpls l2vpn Command Options

Option	Description
l2vpn interface *interface-name*	Sends ping requests out the specified interface configured for the Layer 2 VPN on the outbound (egress) PE router.
l2vpn instance *l2vpn-instance-name* local-site-id *local-site-id-number* remote-site-id *remote-site-id-number*	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.
bottom-label-ttl	(Optional) Displays the time-to-live (TTL) value for the bottom label in the MPLS label stack.
exp *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(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 *source-address*	(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 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 234.

Pinging Layer 2 Circuits

Enter the ping mpls l2circuit command with the following syntax. Table 120 on page 250 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 230.)

Table 120: CLI ping mpls l2circuit Command Options

Option	Description
l2circuit interface *interface-name*	Sends ping requests out the specified interface configured for the Layer 2 circuit on the outbound PE router.
l2circuit virtual-circuit neighbor *prefix-name virtual-circuit-id*	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 *forwarding-class*	(Optional) Specifies the value of the forwarding class to be used in the MPLS ping packets.
count*number*	(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 *source-address*	(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 234.

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 235.)

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 251
- Using the traceroute monitor Command on page 252

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 121 on page 251 describes the traceroute command options.

```
user@host> traceroute host <interface interface-name> <as-number-lookup>
<bypass-routing> <gateway address> <inet | inet6> <no-resolve>
<routing-instance routing-instance-name> <source source-address> <tos number>
<ttl number> <wait seconds>
```

To quit the traceroute command, press Ctrl-C.

Table 121: CLI traceroute Command Options

Option	Description
host	Sends traceroute packets to the hostname or IP address you specify.
interface *interface-name*	(Optional) Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.

Table 121: CLI traceroute Command Options *(continued)*

Option	Description
as-number-lookup	(Optional) Displays the autonomous system (AS) number of each intermediate hop between the router and the destination host.
bypass-routing	(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.
gateway *address*	(Optional) Uses the gateway you specify to route through.
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.
no-resolve	(Optional) Suppresses the display of the hostnames of the hops along the path.
routing-instance *routing-instance-name*	(Optional) Uses the routing instance you specify for the traceroute.
source *address*	(Optional) Uses the source address that you specify, in the traceroute packet.
tos *number*	(Optional) Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255.
ttl *number*	(Optional) Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 128.
wait *seconds*	(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 238.

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 122 on page 253 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 122: CLI traceroute monitor Command Options

Option	Description
host	Sends traceroute packets to the hostname or IP address you specify.
count *number*	(Optional) Limits the number of ping requests, in packets, to send in summary mode. If you do not specify a count, ping requests are continuously sent until you press Q.
inet	(Optional) Forces the traceroute packets to an IPv4 destination.
inet6	(Optional) Forces the traceroute packets to an IPv6 destination.
interval *seconds*	(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 *bytes*	(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 *address*	(Optional) Uses the source address that you specify, in the traceroute packet.
summary	(Optional) Displays the summary traceroute information.

Following is sample output from a traceroute monitor command:

```
user@host> traceroute monitor host2

                                                          My traceroute  [v0.69]
 host (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)
   Wed Mar 14 23:14:11 2007
 Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                                         Packets
          Pings
  Host                                                                                 Loss%   Snt
Last   Avg  Best  Wrst StDev
  1. 173.24.232.66                                                                      0.0%     5
 9.4   8.6   4.8   9.9   2.1
  2. 173.24.232.66                                                                      0.0%     5
 7.9  17.2   7.9  29.4  11.0
  3. 173.24.232.66                                                                      0.0%     5
 9.9   9.3   8.7   9.9   0.5
  4. 173.24.232.66                                                                      0.0%     5
 9.9   9.8   9.5  10.0   0.2
```

Table 123 on page 254 summarizes the output fields of the display.

Table 123: CLI traceroute monitor Command Output Summary

Field	Description
host	Hostname or IP address of the Services Router issuing the traceroute monitor command.
psize*size*	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.
Packets	
number	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

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 124 on page 255 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 124: CLI mtrace from-source Command Options

Option	Description
source *host*	Traces the path to the specified hostname or IP address.
extra-hops *number*	(Optional) Sets the number of extra hops to trace past nonresponsive routers. Specify a value from 0 through 255.
group *address*	(Optional) Traces the path for the specified group address. The default value is 0.0.0.0.
interval *seconds*	(Optional) Sets the interval between statistics gathering. The default value is 10.
max-hops *number*	(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 *number*	(Optional) Sets the maximum number of query attempts for any hop. Specify a value from 1 through 32. The default value is 3.
response *host*	(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 *routing-instance-name*	(Optional) Traces the routing instance you specify.
ttl *number*	(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 *seconds*	(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.

Table 124: CLI mtrace from-source Command Options *(continued)*

Option	Description
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) protocolttl

Table 125 on page 257 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 125: CLI mtrace from-source Command Output Summary

Field	Description
hop-number	Number of the hop (router) along the path.
host	Hostname, if available, or IP address of the router. If the no-resolve option was entered in the command, the hostname is not displayed.
ip-address	IP address of the router.
protocol	Protocol used.
ttl	TTL threshold.
Round trip time *milliseconds* ms	Total time between the sending of the query packet and the receiving of the response packet.
total ttl of *number* 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 126 on page 258 summarizes the output fields of the display.

Table 126: CLI mtrace monitor Command Output Summary

Field	Description
Mtrace *operation-type* at *time-of-day*	■ *operation-type*—Type of multicast trace operation: query or response. ■ *time-of-day*—Date and time the multicast trace query or response was captured.
by	IP address of the host issuing the query.
resp to *address*	*address*—Response destination address.
qid *qid*	*qid*—Query ID number.
packet from *source* to *destination*	■ *source*—IP address of the source of the query or response. ■ *destination*—IP address of the destination of the query or response.
from *source* to *destination*	■ *source*—IP address of the multicast source. ■ *destination*—IP address of the multicast destination.
via group *address*	*address*—Group address being traced.
mxhop=*number*	*number*—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 259
- Using the monitor traffic Command on page 260

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 127 on page 259 and Table 128 on page 259 list the keys you use to control the display using the *interface-name* and traffic options. (The keys are not case sensitive.)

Table 127: 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 show interfaces terse command.
q or ESC	Quits the command and returns to the command prompt.
t	Thaws the display, resuming the update of the statistics and delta counters.

Table 128: 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.

Table 128: CLI monitor interface traffic Output Control Keys *(continued)*

Key	Action
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:                                         Current delta
  Input bytes:                  381588589                         [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 129 on page 261 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 239.

Table 129: CLI monitor traffic Command Options

Option	Description
absolute-sequence	(Optional) Displays the absolute TCP sequence numbers.
count *number*	(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.
interface *interface-name*	(Optional) Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.
layer2-headers	(Optional) Displays the link-layer packet header on each line.
matching "*expression*"	(Optional) Displays packet headers that match an expression enclosed in quotation marks (" "). Table 130 on page 262 through Table 132 on page 264 list match conditions, logical operators, and arithmetic, binary, and relational operators you can use in the expression.
no-domain-names	(Optional) Suppresses the display of the domain name portion of the hostname.
no-promiscuous	(Optional) Specifies *not* 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.
no-resolve	(Optional) Suppresses the display of hostnames.
no-timestamp	(Optional) Suppresses the display of packet header timestamps.
print-ascii	(Optional) Displays each packet header in ASCII format.
print-hex	(Optional) Displays each packet header, except link-layer headers, in hexadecimal format.
size *bytes*	(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.

Table 129: CLI monitor traffic Command Options *(continued)*

Option	Description
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 130 on page 262, enclosed in quotation marks (" "). You can combine match conditions by using the logical operators listed in Table 131 on page 264 (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 132 on page 264 (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in Table 132 on page 264.
- Binary—Expressions that use the binary operators listed in Table 132 on page 264.
- Packet data accessor—Expressions that use the following syntax:

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

  Replace *protocol* with any protocol in Table 130 on page 262. 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 130: CLI monitor traffic Match Conditions

Match Condition	Description
Entity Type	

Table 130: CLI monitor traffic Match Conditions *(continued)*

Match Condition	Description
host [*address* | *hostname*]	Matches packet headers that contain the specified address or hostname. You can preprend any of the following protocol match conditions, followed by a space, to host: arp, ip, rarp, or any of the Directional match conditions.
network *address*	Matches packet headers with source or destination addresses containing the specified network address.
network *address* mask *mask*	Matches packet headers containing the specified network address and subnet mask.
port [*port-number* | *port-name*]	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 *and* destination.
source or destination	Matches packet headers containing the specified source *or* destination.
Packet Length	
less *bytes*	Matches packets with lengths less than or equal to the specified value, in bytes.
greater *bytes*	Matches packets with lengths greater than or equal to the specified value, in bytes.
Protocol	
arp	Matches all ARP packets.
ether	Matches all Ethernet frames.
ether [broadcast | multicast]	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with source or destination.
ether protocol [*address* | (\arp | \ip | \rarp)	Matches Ethernet frames with the specified address or protocol type. The arguments arp, ip, and rarp are also independent match conditions, so they must be preceded with a backslash (\) when used in the ether protocol match condition.
icmp	Matches all ICMP packets.
ip	Matches all IP packets.
ip [broadcast | multicast]	Matches broadcast or multicast IP packets.
ip protocol [*address* | (\icmp | 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 130: CLI monitor traffic Match Conditions *(continued)*

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

Table 131: CLI monitor traffic Logical Operators

<table>
<tr><th>Logical Operator</th><th>Description</th></tr>
<tr><td>!</td><td>Logical NOT. If the first condition does not match, the next condition is evaluated.</td></tr>
<tr><td>&&</td><td>Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.</td></tr>
<tr><td>||</td><td>Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.</td></tr>
<tr><td>()</td><td>Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).</td></tr>
</table>

Table 132: CLI monitor traffic Arithmetic, Binary, and Relational Operators

<table>
<tr><th>Operator</th><th>Description</th></tr>
<tr><td colspan="2">Arithmetic Operator</td></tr>
<tr><td>+</td><td>Addition operator.</td></tr>
<tr><td>–</td><td>Subtraction operator.</td></tr>
<tr><td>/</td><td>Division operator.</td></tr>
<tr><td colspan="2">Binary Operator</td></tr>
<tr><td>&</td><td>Bitwise AND.</td></tr>
<tr><td>*</td><td>Bitwise exclusive OR.</td></tr>
<tr><td>|</td><td>Bitwise inclusive OR.</td></tr>
<tr><td colspan="2">Relational Operator</td></tr>
<tr><td><=</td><td>A match occurs if the first expression is less than or equal to the second.</td></tr>
<tr><td>>=</td><td>A match occurs if the first expression is greater than or equal to the second.</td></tr>
<tr><td><</td><td>A match occurs if the first expression is less than the second.</td></tr>
<tr><td>></td><td>A match occurs if the first expression is greater than the second.</td></tr>
<tr><td>=</td><td>A match occurs if the first expression is equal to the second.</td></tr>
</table>

Table 132: CLI monitor traffic Arithmetic, Binary, and Relational Operators *(continued)*

Operator	Description
!=	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 13

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 239.

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

Before configuring packet capture on a Services Router, become familiar with the terms defined in Table 133 on page 268.

Table 133: 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	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 /var/tmp 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. *See also traffic sampling*. 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 239).
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. See also *packet capture*.

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

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 273.

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 276.

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 273.

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 275.

For more details about analyzing packet capture files, see Verifying Captured Packets on page 278.

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 268.

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 271
- Configuring Packet Capture on an Interface (Required) on page 273
- Configuring a Firewall Filter for Packet Capture (Optional) on page 273
- Disabling Packet Capture on page 275
- Deleting Packet Capture Files on page 275

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 134 on page 272.
3. Go on to "Configuring Packet Capture on an Interface (Required)" on page 273.

Table 134: Enabling Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Forwarding options** level in the configuration hierarchy.	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**. In the configuration editor hierarchy, select **Forwarding options**.	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.	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. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	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.	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 135 on page 273.
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 273.
   - To check the configuration, see "Verifying Packet Capture" on page 277.

Table 135: Configuring Packet Capture on an Interface

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Interfaces** level in the configuration hierarchy, and select an interface for packet capture—for example, fe-0/0/1. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	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.	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 136 on page 274.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see "Verifying Packet Capture" on page 277.

Table 136: Configuring a Firewall Filter for Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Firewall** level in the configuration hierarchy.	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.	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 set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
Apply the dest-all filter to all the outgoing packets on the interface—for example, fe-0/0/1.0. (See the interface naming conventions in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.)	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.	

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 137 on page 275.
3. If you are finished configuring the router, commit the configuration.

Table 137: Disabling Packet Capture

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Forwarding options** level in the configuration hierarchy.	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.	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 275.
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 271.
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 275.
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 271.
7. Commit the configuration.

Verifying Packet Capture

To verify packet capture, perform these tasks:

- Displaying a Packet Capture Configuration on page 277
- Displaying a Firewall Filter for Packet Capture Configuration on page 278
- Verifying Captured Packets on page 278

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.

```
[edit]
user@host# show forwarding-options
packet-capture {
   file filename pcap-file files 100 size 1024;
   maximum-capture-size 500;
}
```

What It Means Verify that the output shows the intended file configuration for capturing packets.

Related Topics For more information about the format of a configuration file, see the information about viewing configuration text in the *J-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.

```
[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.

Related Topics 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 275.
- 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.

```
root@server% tcpdump -r 126b.fe-0.0.1 -xevvvv
01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl  64, id 33133, offset 0, flags [none], proto: ICMP (1),
 length: 84) 14.1.1.1 > 15.1.1.1: ICMP echo request seq 0, length 64
                         0005 85c8 f6d1 0005 85c4 e3d1 0800 4500
                         0054 816d 0000 4001 da38 0e01 0101 0f01
                         0101 0800 3c5a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
01:12:36.279793 Out 0:5:85:c8:f6:d1 > 0:5:85:c4:e3:d1, ethertype IPv4 (0x0800),
length 98: (tos 0x0, ttl  63, id 41227, offset 0, flags [none], proto: ICMP (1),
 length: 84) 15.1.1.1 > 14.1.1.1: ICMP echo reply seq 0, length 64
                         0005 85c4 e3d1 0005 85c8 f6d1 0800 4500
                         0054 a10b 0000 3f01 bb9a 0f01 0101 0e01
                         0101 0000 445a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
root@server%
```

What It Means Verify that the output shows the intended packets.

Chapter 14

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

Before configuring and monitoring RPM on J-series Services Routers, become familiar with the terms defined in Table 138 on page 281.

Table 138: RPM Terms

Term	Definition
egress	Outbound. Characterizing packets exiting a Services Router.
ingress	Inbound. Characterizing packets entering a Services Router.
jitter	Difference in relative transmit time between two consecutive packets in a stream, which can cause quality degradation in some real-time applications such as voice over IP (VoIP) and video.
probe	An action taken or an object used to learn something about the state of the network. Real-time performance monitoring (RPM) uses several types of requests to probe a network.
probe interval	Time, in seconds, between probe packets.

Table 138: 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

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 has been sent and the corresponding responses received, the test is complete. You can manually set the probe interval for each test to control how the RPM test is conducted.

After all the probes for a particular test have been sent, the test begins again. The time between tests is the test interval. You can manually set the test interval to tune RPM performance.

Jitter Measurement with Hardware Timestamping

Jitter is the difference in relative transit time between two consecutive probes.

You can timestamp the following RPM probes to improve the measurement of latency or jitter:

- ICMP ping
- ICMP ping timestamp
- UDP ping
- UDP ping timestamp

NOTE: The Services Router supports hardware timestamping of UDP ping and UDP ping timestamp RPM probes only if the destination port is UDP-ECHO (port 7).

Timestamping takes place during the forwarding process of the Services Router originating the probe (the RPM client), but not on the remote router that is the target of the probe (the RPM server).

The supported encapsulations on a Services Router for timestamping are Ethernet including VLAN, synchronous PPP, and Frame Relay. The only logical interface supported is an lt services interface.

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 139 on page 284.

Table 139: 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
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

Table 139: RPM Statistics *(continued)*

RPM Statistics	Description
Ingress jitter	Difference between the maximum and minimum inbound times, as measured over the course of the test
Probe Counts	
Probes sent	Total number of probes sent over the course of the test
Probe responses received	Total number of probe responses received over the course of the test
Loss percentage	Percentage of probes sent for which a response was not received

RPM Thresholds and Traps

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

If the result of a probe or test exceeds any threshold, the 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 49.

Configuring RPM with Quick Configuration

J-Web Quick Configuration allows you to configure real-time performance monitoring (RPM) parameters. Figure 27 on page 286 shows the main Quick Configuration page for RPM. Figure 28 on page 287 shows the probe test Quick Configuration page for RPM.

Figure 27: Main Quick Configuration Page for RPM

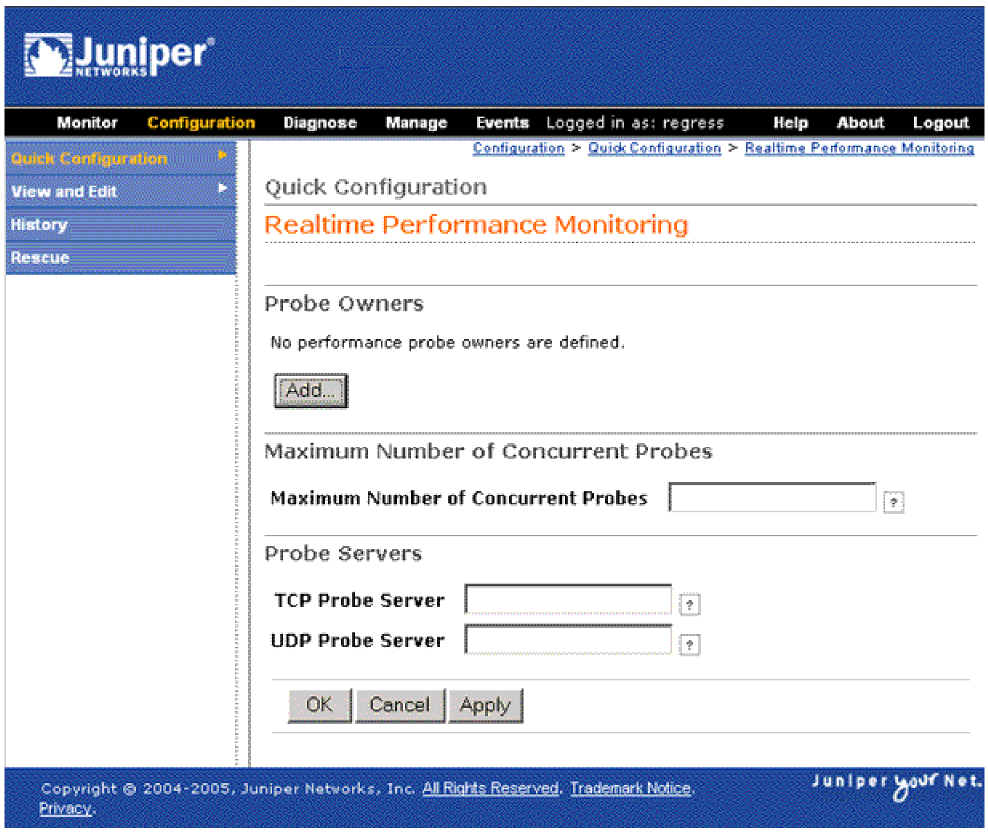
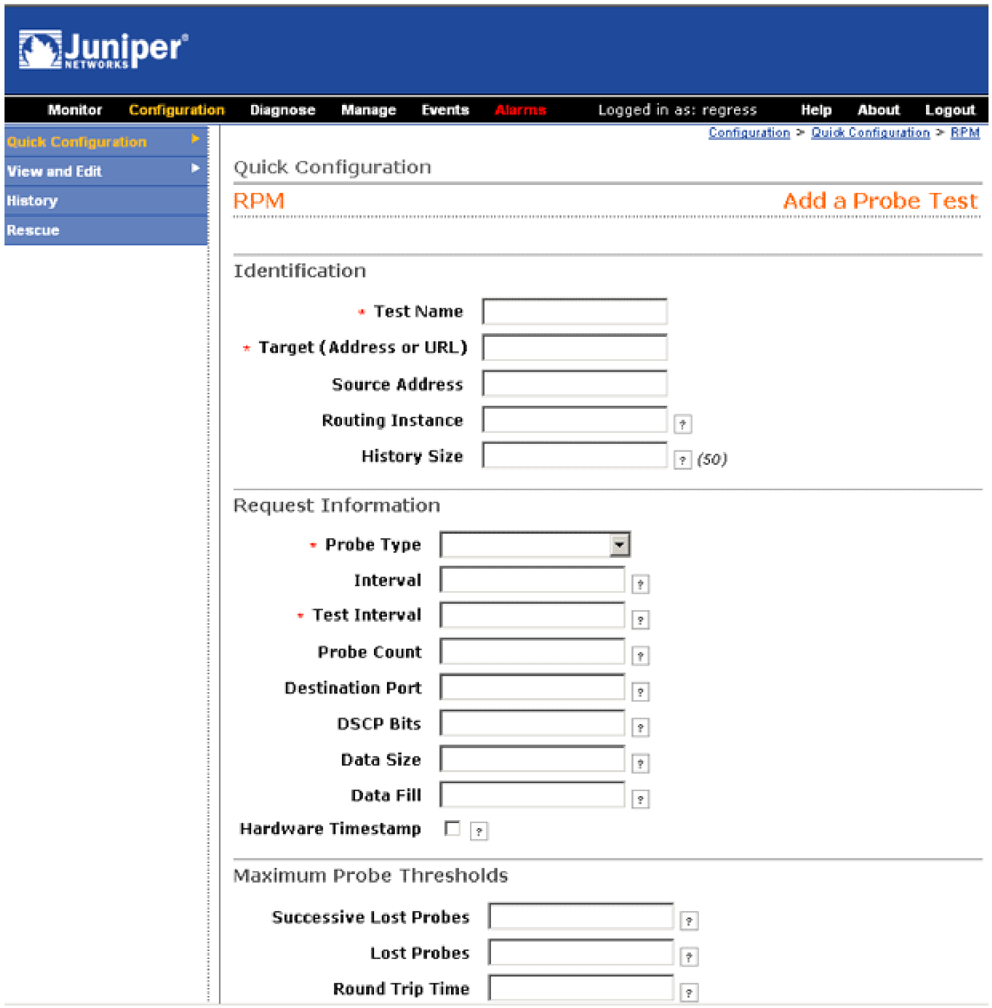


Figure 28: Probe Test Quick Configuration Page for RPM



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 140 on page 288.
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 301.

Table 140: 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		
Probe Type (required)	Specifies the type of probe to send as part of the test.	Select the desired probe type from the list: ■ **http-get** ■ **http-get-metadata** ■ **icmp-ping** ■ **icmp-ping-timestamp** ■ **tcp-ping** ■ **udp-ping**
Interval	Sets the wait time (in seconds) between each probe transmission	Type a number between 1 and 255 (seconds).
Test Interval (required)	Sets the wait time (in seconds) between tests.	Type a number between 0 and 86400 (seconds).
Probe Count	Sets the total number of probes to be sent for each test.	Type a number between 1 and 15.

Table 140: RPM Quick Configuration Summary *(continued)*

Field	Function	Your Action
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server (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.	Type the number 7—a standard TCP or UDP port number—or a port number from 49152 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6–bit pattern. The default is 000000. For information about DSCPs and their use within class-of-service (CoS) features, see the *J-series Services Router Advanced WAN Access Configuration Guide*.	Type a valid 6–bit pattern.
Data Size	Specifies the size of the data portion of the ICMP probes.	Type a size (in bytes) between 0 and 65507.
Data Fill	Specifies the contents of the data portion of the ICMP probes.	Type a hexadecimal value between 1 and 800h to use as the contents of the ICMP probe data.
Hardware Timestamp	Enables timestamping of RPM probe messages. On J-series Services Routers you can timestamp the following RPM probes to improve the measurement of latency or jitter: ■ ICMP ping ■ ICMP ping timestamp ■ UDP ping—destination port UDP-ECHO (port 7) only ■ UDP ping timestamp—destination port UDP-ECHO (port 7) only	To enable timestamping, select the check box.
Maximum Probe Thresholds		
Successive Lost Probes	Sets the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Lost Probes	Sets the total number of probes that must be lost to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Round Trip Time	Sets the total round-trip time (in microseconds), from the 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).

Table 140: RPM Quick Configuration Summary *(continued)*

Field	Function	Your Action
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Sets the total one-way time (in microseconds), from the 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		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	■ 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.	■ 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.	■ 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.	■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.

Table 140: RPM Quick Configuration Summary *(continued)*

Field	Function	Your Action
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	■ 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.	■ 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.	■ 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.	■ 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.	■ 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.	■ To enable SNMP traps for this condition, select the check box. ■ To disable SNMP traps, clear the check box.
Test Completion	Generates traps when a test is completed.	■ 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.	■ 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

To configure basic RPM probes, you must configure the probe owner, the test, and the specific parameters of the RPM probe.

For ICMP ping, ICMP ping timestamp, UDP ping, and UDP ping timestamp probes, you can also set a timestamp to improve the measurement of latency or jitter. The probe is timestamped by the router originating the probe (the RPM client).

In this sample use of RPM, basic probes are configured for two customers: Customer A and Customer B. The probe for Customer A uses ICMP timestamp packets and sets RPM thresholds and corresponding SNMP traps to catch lengthy inbound times. The probe for Customer B uses HTTP packets and sets thresholds and corresponding SNMP traps to catch excessive lost probes. To configure these RPM probes:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 141 on page 293.
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 295.
   - To tune a probe, see “Tuning RPM Probes” on page 297.
   - To check the configuration, see “Verifying an RPM Configuration” on page 301.

Table 141: Configuring Basic RPM Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Services > RPM** level in the configuration hierarchy.	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.	1. In the Probe box, click **Add new entry**. 2. In the Owner box, type customerA. 3. Click **OK**. 4. Repeat the previous steps and add an RPM probe owner for customerB.	1. Enter set probe customerA 2. Enter set probe customerB
Configure the RPM test icmp-test for the RPM owner customerA. The sample RPM test is an ICMP probe with a test interval (probe frequency) of 15 seconds, a probe type of icmp-ping-timestamp, a probe timestamp, and a target address of 192.178.16.5.	1. On the Rpm page, select **customerA**. 2. In the Test box, click **Add new entry** 3. In the Name box, type icmp-test. 4. In the Test interval box, type 15. 5. In the Probe type box, select **icmp-ping-timestamp**. 6. Select the **Hardware timestamp** check box. 7. In the Target box, select the **Yes** check box, and click **Configure**. 8. In the Target type box, select **Address**. 9. In the Address box, type 192.178.16.5. 10. Click **OK**.	1. From the [edit] hierarchy level, enter edit services rpm probe customerA 2. Enter set test icmp-test probe-frequency 15 3. Enter set test icmp-test probe-type icmp-ping-timestamp 4. Enter set test icmp-test hardware-timestamp 5. Enter set test icmp-test target address 192.178.16.5

Table 141: Configuring Basic RPM Probes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.	1. On the Probe page, select **icmp-test**. 2. In the Thresholds box, select the **Yes** check box, and click **Configure**. 3. In the Ingress time box, type 3000. 4. Click **OK**. 5. In the Traps box, click **Add new entry**. 6. In the Value box, select **ingress-time-exceeded**. 7. Click **OK**.	1. Enter set probe customerA test icmp-test thresholds ingress-time 3000 2. Enter set probe customerA test icmp-test traps ingress-time-exceeded
Configure the RPM test http-test for the RPM owner customerB. 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.	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**.	1. From the [edit] hierarchy level, enter edit services rpm probe customerB 2. Enter set test http-test probe-frequency 30 3. Enter set test http-test probe-type http-get 4. Enter set test http-test target url http://customerB.net

Table 141: Configuring Basic RPM Probes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure RPM thresholds and corresponding SNMP traps to catch 3 or more successive lost probes and total lost probes of 10 or more.	1. On the Probe page, select **http-test**. 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**.	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.

If you are using class of service (CoS) and want to classify probes, you must also set a destination interface. The destination interface is the output interface for sending packets to the forwarding plane. Classified packets are sent to the output queue on the output interface specified by the CoS scheduler map configured on the interface.

For information about CoS, see the *J-series Services Router Advanced WAN Access Configuration Guide*.

CAUTION: Use probe classification with caution, because improper configuration can cause packets to be dropped.

The destination interface must support looping of probe packets to an input interface without adding any encapsulation. On a Services Router, the destination interface must be an lt services interface.

In this sample use of RPM, a probe is configured for one customer: Customer C. The probe for Customer C uses TCP packets. The remote router is configured as an RPM server for both TCP and UDP packets, using an lt services interface as the destination interface, and ports 50000 and 50037, respectively. 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 142 on page 296.
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 297.
   - To check the configuration, see "Verifying an RPM Configuration" on page 301.

Table 142: 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.	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.	1. In the Probe box, click **Add new entry**. 2. In the Owner box, type customerC. 3. Click **OK**.	Enter set probe customerC
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.	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**.	1. From the [edit] hierarchy level, enter edit services rpm probe customerC 2. Enter set test tcp-test probe-frequency 5 3. Enter set test tcp-test probe-type tcp-ping 4. Enter set test tcp-test target address 192.162.45.6

Table 142: Configuring TCP and UDP Probes *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the destination interface. **NOTE:** On Services Routers the destination interface must be an lt services interface.	In the Destination interface box, type lt-0/0/0	Enter set test tcp-test destination-interface lt-0/0/0
Configure port 50000 as the TCP port to which the RPM probes are sent.	In the Destination port box, type 50000.	Enter set test tcp-test destination-port 50000
Router B Configuration		
Navigate to the **Services > RPM** level in the configuration hierarchy.	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.	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.	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 292.

To configure tune RPM probes:

1. Perform the configuration tasks described in Table 141 on page 293.
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 143 on page 298.
4. If you are finished configuring the network, commit the configuration.
5. To check the configuration, see “Verifying an RPM Configuration” on page 301.

Table 143: Tuning RPM Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Services > RPM** level in the configuration hierarchy.	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.	1. In the Probe limit box, type 10. 2. Click **OK**.	Enter set probe-limit 10
Access the ICMP probe of customer A.	1. In the Owner box, click **CustomerA**. 2. In the Name box, click **icmp-test**.	From the [edit] hierarchy level, enter edit services rpm probe customerA test icmp-test
Set the time between probe transmissions to 15 seconds.	In the Probe interval box, type 15.	Enter set probe-interval 15
Set the number of probes within a test to 10.	In the Probe count box, type 10.	Enter set probe-count 10
Set the source address for each probe packet to 192.168.2.9. 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.	1. In the Source address box, type 192.168.2.9. 2. Click **OK**.	Enter set source-address 192.168.2.9

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

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 144 on page 299.
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 300.
   - To check the configuration, see "Verifying an RPM Configuration" on page 301.

Table 144: 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.	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

Table 144: Configuring RPM Probes to Monitor BGP Neighbors *(continued)*

Task	J-Web Configuration Editor	CLI Configuration Editor
Specify the number of probe results to be saved in the probe history—for example, 25. The range is between 0 and 255, and the default is 50.	In the History size box, type 25.	Enter set history-size 25
Configure the probe count—for example, 5—and probe interval—for example, 1. ■ 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.	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.	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.

The sample RPM configuration in Table 145 on page 301 sends RPM probes to the BGP neighbors in routing instance R1.

To direct RPM probes to select BGP neighbors:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 145 on page 301.
3. If you are finished configuring the router, commit the configuration.
4. To verify the configuration, see “Verifying an RPM Configuration” on page 301.

Table 145: 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**. 2. Next to Services, click **Configure** or **Edit**. 3. Next to Rpm, select the **Yes** check box and click **Configure** or **Edit**. 4. Next to Bgp, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit services rpm bgp
Configure routing instance RI1 to send RPM probes to BGP neighbors within the routing instance.	1. Next to Routing instances, click **Add new entry**. 2. In the Routing instance name box, type RI1. 3. Click **OK**.	Enter set routing-instances RI1

Verifying an RPM Configuration

To verify an RPM configuration, perform these tasks:

- Verifying RPM Services on page 301
- Verifying RPM Statistics on page 302
- Verifying RPM Probe Servers on page 303

Verifying RPM Services

Purpose Verify that the RPM configuration is within the expected values.

Action From configuration mode in the CLI, enter the show services rpm command.

```
user@host# show services rpm
   probe test {
    test customerA {
        probe-type icmp-ping;
        target address 192.178.16.5;
        probe-count 15;
        probe-interval 1;
        hardware-timestamp;
    }
    test customerB {
        probe-type icmp-ping-timestamp;
        target address 192.178.16.5;
        probe-count 15;
        probe-interval 1;
        hardware-timestamp;
    }
    test customerC {
```

```
      probe-type udp-ping;
      target address 192.178.16.5;
      probe-count 15;
      probe-interval 1;
      destination-port 50000;
      hardware-timestamp;
  }
 }
```

What It Means The output shows the values that are configured for RPM on the Services Router.

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 show services rpm probe-results command.

```
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
```

What It Means The output shows the probe results for the RPM tests configured on the Services Router. Verify the following information:

- Each configured test is displayed. Results are displayed in alphabetical order, sorted first by owner name and then by test name.
- The round-trip times fall within the expected values for the particular test. The minimum round-trip time is displayed as Minimum Rtt, the maximum round-trip time is displayed as Maximum Rtt, and the average round-trip time is displayed as Average Rtt.

  A high average round-trip time might mean that performances problems exist within the network. A high maximum round-trip time might result in high jitter values.
- The egress (outbound) trip times fall within the expected values for the particular test. The minimum outbound time is displayed as Minimum egress time, the maximum outbound time is displayed as Maximum egress time, and the average outbound time is displayed as Average egress time.
- The ingress (inbound) trip times fall within the expected values for the particular test. The minimum inbound time is displayed as Minimum ingress time, the maximum inbound time is displayed as Maximum ingress time, and the average inbound time is displayed as Average ingress time.
- The number of probes sent and received is expected.

  Lost probes might indicate packet loss through the network. Packet losses can occur if the remote server is flapping. If the RPM probe type is TCP or UDP, complete probe loss might indicate a mismatch in TCP or UDP RPM port number.
- For Type, each peer is configured as the correct type (either internal or external).

Related Topics For a complete description of show services rpm probe-results output, see the *JUNOS System Basics and Services Command Reference*.

Verifying RPM Probe Servers

Purpose Verify that the Services Router is configured to receive and transmit TCP and UDP RPM probes on the correct ports.

Action From the CLI, enter the show services rpm active-servers command.

```
user@host> show services rpm active-servers
    Protocol: TCP, Port: 50000

    Protocol: UDP, Port: 50037
```

What It Means The output shows a list of the protocols and corresponding ports for which the Services Router is configured as an RPM server.

Related Topics For a complete description of show services rpm active-servers output, see the *JUNOS System Basics and Services Command Reference*.

Part 5
Index

Index

E

U

V

W

X

Y