J-series™ Services Router

Administration Guide

Release 7.2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, California 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-013029-01, Revision 1

J-series™ Services Router Administration Guide, Release 7.2
Copyright © 2005, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Michael Bushong, Taffy Everts, Jerry Isaac, Archana Maheshwari, Laura Phillips, Frank Reade, and Swapna Steiger
Editing: Taffy Everts and Stella Hackell
Illustration: Faith Bradford Brown and Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
13 April 2005—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.

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 Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.

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.

c. Other Juniper documentation for the Software (such as product purchase documents, documents accompanying the product, the Software user manual(s), Juniper's website for the Software, or messages displayed by the Software) may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, concurrent users, sessions, subscribers, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, or capabilities, or provide temporal or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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, 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; (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, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, 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 Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation 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; or (k) 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.

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.** If the Software is distributed on physical media (such as CD), Juniper warrants for 90 days from delivery that the media on which the Software is delivered will be free of defects in material and workmanship under normal use. This limited warranty extends only to the Customer. Except as may be expressly provided in separate documentation from Juniper, no other warranties apply to the Software, and the Software is otherwise provided AS IS. Customer assumes all risks arising from use of the Software. Customer's sole remedy and Juniper's entire liability under this limited warranty is that Juniper, at its option, will repair or replace the media containing the Software, or provide a refund, provided that Customer makes a proper warranty claim to Juniper, in writing, within the warranty period. Nothing in this Agreement shall give rise to any obligation to support the Software. Any such support shall be governed by a separate, written agreement. To the maximum extent permitted by law, Juniper shall not be liable for any liability for 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 HEREIN OR IN SEPARATE DOCUMENTATION PROVIDED FROM JUNIPER AND 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.

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 you may contain encryption or other capabilities restricting your 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. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. 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.

If you have any questions about this agreement, contact Juniper Networks at the following address:

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
Attn: Contracts Administrator

Abbreviated Table of Contents

Table of Contents

About This Guide

This preface provides the following guidelines for using this manual and related Juniper Networks, Inc., technical documents:

Objectives

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

NOTE: This guide documents Release 7.2 of the JUNOS software. For additional information about J-series Services Routers—either corrections to or omissions from this guide—see the *J-series Services Router Release Notes* at http://www.juniper.net.

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

Table 1: Capabilities of J-series Interfaces

J-series Interface	Capabilities
J-Web graphical browser interface	■ Quick (basic) configuration ■ Monitoring, configuration, diagnosis, and management
JUNOS CLI	Monitoring, configuration, diagnosis, and management

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

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

Because you can configure and manage a Services Router in several ways, most chapters in J-series Services Router guides contain multiple sets of instructions:

- Configuration—For many Services Router features, you can use J-Web Quick Configuration for basic setup. For more extensive configuration of all Services Router features, use the J-Web configuration editor or the JUNOS CLI configuration editor.
- Maintenance—To monitor, diagnose, and manage a Services Router, use the J-Web interface for common tasks, or use CLI operational mode commands.

J-series Services Routers are documented in three guides. Table 2 shows where Services Router instructions are located.

Table 2: Location of Tasks in J-series Guides

Services Router Tasks	Location of Instructions
Installing hardware and establishing basic connectivity	*J-series Services Router Getting Started Guide*
Configuring interfaces and routing protocols	*J-series Services Router Configuration Guide*
Managing users and operations, monitoring performance, upgrading software, and diagnosing common problems	*J-series Services Router Administration Guide*

Document Conventions

Table 3 defines the notice icons used in this guide.

Table 3: Notice Icons

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

Table 4 defines the text and syntax conventions used in this guide.

Table 4: Text and Syntax Conventions

Convention	Description	Examples
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width typeface`	Represents output that appears on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic typeface	■ 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*

Convention	Description	Examples
Italic sans serif typeface	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*
Sans serif typeface	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 typeface	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 three 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 5.

Table 5: J-series Guides and Related JUNOS Software Publications

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
J-series Services Router Getting Started Guide	
"J-series User Interface Overview" "Establishing Basic Connectivity" "Configuring Autoinstallation"	*JUNOS System Basics Configuration Guide*
J-series Services Router Configuration Guide	
"Using J-series Configuration Tools"	*JUNOS System Basics Configuration Guide*
"Configuring Network Interfaces" "Configuring Point-to-Point Protocol over Ethernet"	■ *JUNOS Network Interfaces and Class of Service Configuration Guide* ■ *JUNOS Network and Services Interfaces Command Reference*
"Routing Overview" "Configuring Static Routes" "Configuring a RIP Network" "Configuring an OSPF Network" "Configuring BGP Sessions"	■ *JUNOS Routing Protocols Configuration Guide* ■ *JUNOS Protocols, Class of Service, and System Basics Command Reference*
"Multiprotocol Label Switching Overview" "Configuring Signaling Protocols for Traffic Engineering" "Configuring Virtual Private Networks"	■ *JUNOS MPLS Applications Configuration Guide* ■ *JUNOS Routing Protocols Configuration Guide* ■ *JUNOS VPNs Configuration Guide*
"Configuring IPSec for Secure Packet Exchange"	■ *JUNOS System Basics Configuration Guide* ■ *JUNOS Services Interfaces Configuration Guide* ■ *JUNOS Network and Services Interfaces Command Reference*
"Multicast Overview" "Configuring a Multicast Network"	*JUNOS Multicast Protocols Configuration Guide*
"Policy, Firewall Filter, and Class-of-Service Overview" "Configuring Routing Policies"	*JUNOS Policy Framework Configuration Guide*
"Configuring Firewall Filters and NAT"	■ *JUNOS Network Interfaces and Class of Service Configuration Guide* ■ *JUNOS Policy Framework Configuration Guide* ■ *JUNOS Services Interfaces Configuration Guide*

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
"Configuring Class of Service with DiffServ"	■ *JUNOS Network Interfaces and Class of Service Configuration Guide* ■ *JUNOS Protocols, Class of Service, and System Basics Command Reference*
J-series Services Router Administration Guide	
"Managing Users and Operations"	*JUNOS System Basics Configuration Guide*
"Configuring SNMP for Network Management"	*JUNOS Network Management Configuration Guide*
"Configuring the DHCP Server"	*JUNOS System Basics Configuration Guide*
"Configuring and Monitoring Alarms"	*JUNOS System Basics Configuration Guide*
"Monitoring and Diagnosing a Services Router"	■ *JUNOS Protocols, Class of Service, and System Basics Command Reference* ■ *JUNOS Network and Services Interfaces Command Reference*
"Monitoring Real-Time Performance"	*JUNOS Network and Services Interfaces 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
Administration Tasks

Chapter 1

Installing and Managing J-series Licenses

To enable some JUNOS software features and use additional ports on a J-series Services Router, you must purchase, install, and manage separate software licenses. The presence on the router of the appropriate software license keys (passwords) determines the features and ports you can configure and use.

For information about how to purchase J-series software licenses, contact your Juniper Networks sales representative.

This chapter contains the following topics:

J-series License Overview

The J-series set of licenses is composed of two primary types: feature licenses and port licenses. Each type of license is valid for only a single Services Router. To manage the licenses, you must understand the components of a license key.

This section contains the following topics:

Software Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one Services Router. Table 6 lists the Services Router software features that require licenses.

Table 6: J-series Services Router Software Feature Licenses

Licensed Software Feature	License Name
Stateful Firewall Filters and NAT	
Stateful firewall and Network Address Translation (NAT) on the J2300 platform—all configuration statements within the [edit services stateful-firewall] hierarchy.	J2300 Services Router Software License for Stateful Firewall
Stateful firewall and NAT on the J4300 platform—all configuration statements within the [edit services stateful-firewall] hierarchy.	J4300 Services Router Software License for Stateful Firewall
Stateful firewall and NAT on the J6300 platform—all configuration statements within the [edit services stateful-firewall] hierarchy.	J6300 Services Router Software License for Stateful Firewall
IPSec VPN Tunneling	
IPSec VPN tunneling on the J2300 platform—all configuration statements within the [edit services ipsec-vpn] hierarchy.	J2300 Services Router Software License for IPSec Tunneling
IPSec VPN tunneling on the J4300 platform—all configuration statements within the [edit services ipsec-vpn] hierarchy.	J4300 Services Router Software License for IPSec Tunneling
IPSec VPN tunneling on the J6300 platform—all configuration statements within the [edit services ipsec-vpn] hierarchy.	J6300 Services Router Software License for IPSec Tunneling
Traffic Analysis	
J-Flow traffic analysis—all configuration statements within the [edit forwarding-options sampling] and [edit forwarding-options accounting] hierarchies.	J-series Services Router Software License for J-Flow Traffic Analysis
BGP Route Reflectors	
Advanced Border Gateway Protocol (BGP) features that enable route reflectors—all configuration statements within the [edit protocols bgp cluster] hierarchy. BGP clusters allow routers to act as route reflectors by enabling the readvertising of BGP routes to internal peers.	J-series Services Router Software License for Advanced Border Router Protocol Support

Port Licenses

Each port license is tied to exactly one licensed port, and that license is valid for exactly one Services Router. To enable multiple ports, you must have a license for each licensed port.Table 7 lists the additional Services Router port licenses.

Table 7: J-series Services Router Port Licenses

Licensed Port	License Name
T1	
Additional port on a T1 Physical Interface Module (PIM).	J-series Services Router Software License for One Additional T1 Port
E1	
Additional port on an E1 PIM.	J-series Services Router Software License for One Additional E1 Port
Serial	
Additional port on a serial PIM.	J-series Services Router Software License for One Additional Serial Port
Fast Ethernet	
Additional port on a Fast Ethernet PIM.	J-series Services Router Software License for One Additional Fast Ethernet Port

The LAN ports (fe-0/0/0 and fe-0/0/1) do not require port licenses.

Additionally, one port per PIM can be configured without a port license. A port license is required only if you configure more than one port on a particular PIM.

License Key Components

A license key consists of two parts:

- License ID—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- License data—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string li29183743 is the license ID, and the trailing block of data is the license data:

```
li29183743 4ky27y acasck 82fsj6 jzsn4q ix8i8d adj7kr
                  8uq38t ix8i8d jzsn4q ix8i8d 4ky27y acasck
                  82fsj6 ii8i7e adj7kr 8uq38t ks2923 a9382e
```

The license data defines the device ID for which the license is valid and the version of the license.

Before You Begin

Before you begin managing the J-series licenses, complete the following tasks:

- Purchase the licenses you require.
- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.

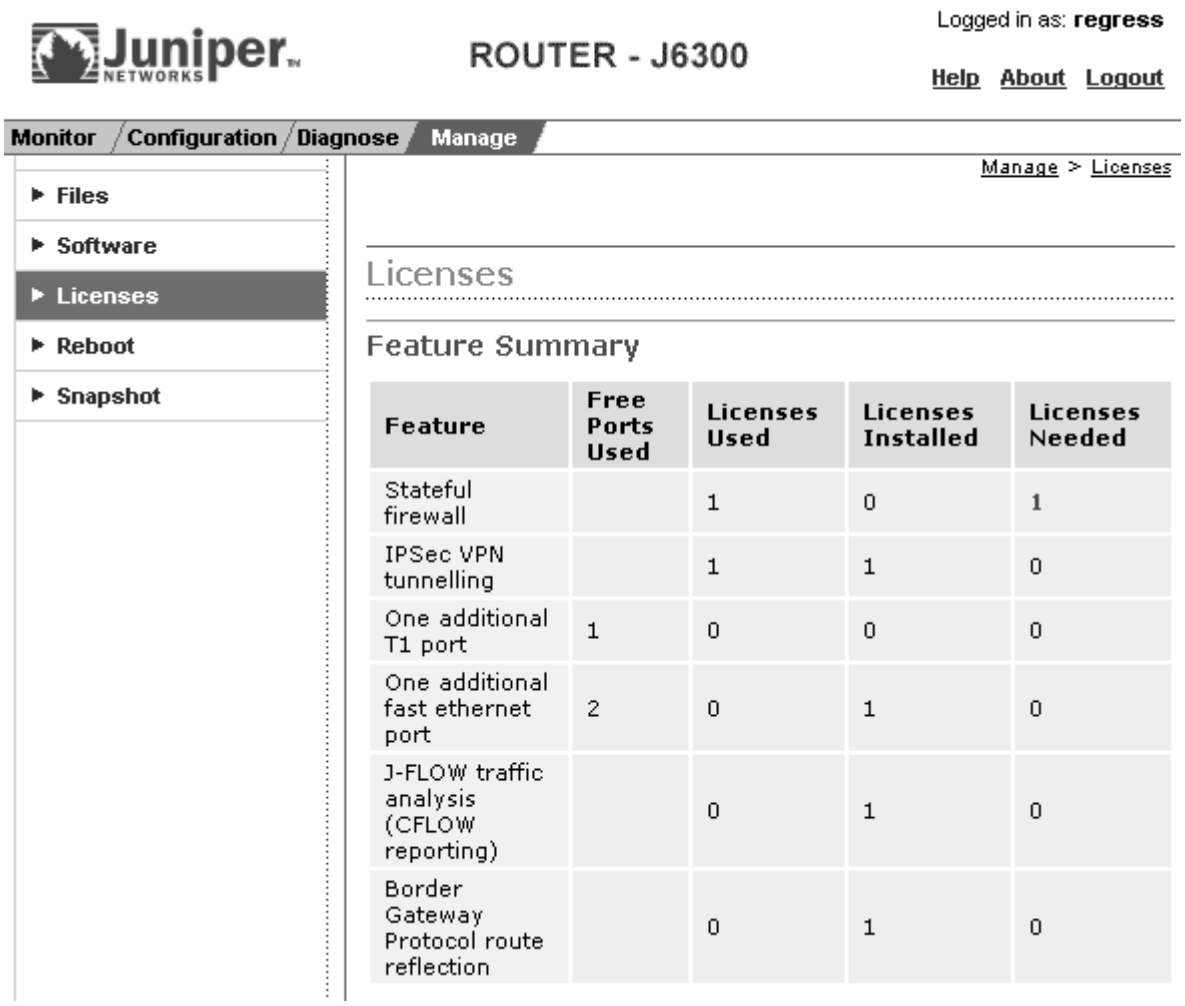
Managing J-series Licenses with the J-Web Interface

To manage licenses with the J-Web interface, you perform the following tasks:

- Adding New Licenses with the J-Web Interface on page 8
- Deleting Licenses with the J-Web Interface on page 9
- Displaying License Keys with the J-Web Interface on page 9
- Downloading Licenses with the J-Web Interface on page 9

Figure 1 shows the J-Web Licenses page.

Figure 1: Licenses Page



The Licenses page displays a summary of licensed features that are configured on the Services Router and a list of the licenses that are installed on the router. The information on the license management page is summarized in Table 8.

Table 8: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	Name of the licensed feature or port: ■ J-series licenses listed in Table 6 and Table 7 ■ All features—All-inclusive licenses

Field Name	Definition
Free Ports Used	If the feature is an interface, this field lists the number of free ports for that interface that are currently configured. If the feature is not an interface, this field is blank.
Licenses Used	Number of licenses currently being used on the router. Usage is determined by the configuration on the router. If a port license exists and that port is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the router for the particular feature or port.
Licenses Needed	Number of licenses required for legal of use the feature or port. Usage is determined by the configuration on the router: ■ If a feature is configured and the license for that feature is not installed, a single license is needed. ■ If one or more ports are configured beyond the number of licenses installed on the router, a single license is needed for each additional configured port.
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	Valid—The installed license key is valid. Invalid—The installed license key is not valid.
Version	Numeric version number of the license key.
Group	If the license defines a group license, this field displays the group definition. If the license requires a group license, this field displays the required group definition. **NOTE:** Because group licenses are currently unsupported, this field is always blank.
Enabled Features	Name of the feature that is enabled with the particular license.

Adding New Licenses with the J-Web Interface

To add a new license key on a Services Router with the J-Web license manager:

1. In the J-Web interface, select **Manage > Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do *one* of the following, using a blank line to separate multiple license keys:
   - In the License File URL box, type the full URL to the destination file containing the license key to be added.

- In the License Key Text box, paste the license key text, in plain-text format, for the license to be added.

4. Click **OK** to add the license key.
5. Go on to "Verifying J-series License Management" on page 11.

Deleting Licenses with the J-Web Interface

To delete one or more license keys from a Services Router with the J-Web license manager:

1. In the J-Web interface, select **Manage > Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.
4. Go on to "Verifying J-series License Management" on page 11.

Displaying License Keys with the J-Web Interface

To display the license keys installed on a Services Router with the J-Web license manager:

1. In the J-Web interface, select **Manage > Licenses**.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the router.

   A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.
3. Go on to "Verifying J-series License Management" on page 11.

Downloading Licenses with the J-Web Interface

To download the license keys installed on the Services Router with the J-Web license manager:

1. In the J-Web interface, select **Manage > Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the router to a single file.
3. Select **Save it to disk** and specify the file to which the license keys are to be written.
4. Go on to "Verifying J-series License Management" on page 11.

Managing J-series Licenses with the CLI

To manage the J-series licenses with the CLI, perform the following tasks.

- Adding New Licenses with the CLI on page 10
- Deleting a License with the CLI on page 10
- Saving License Keys with the CLI on page 11

Adding New Licenses with the CLI

To add a new license key to the Services Router with the CLI:

1. Enter operational mode in the CLI.
2. Enter one of the following CLI commands:
   - To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

     request system license add *filename* | *url*

   - To add a license key from the terminal, enter the following command:

     request system license add terminal
3. When prompted, enter the license key, separating multiple license keys with a blank line.

   If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.
4. Go on to "Verifying J-series License Management" on page 11.

Deleting a License with the CLI

To delete a license key from the Services Router with the CLI:

1. Enter operational mode in the CLI.
2. Enter the following command for each license, specifying the license ID. You can delete only one license at a time.

   request system license delete *license-id*
3. Go on to "Verifying J-series License Management" on page 11.

Saving License Keys with the CLI

To save the licenses installed on the Services Router to a file with the CLI:

1. Enter operational mode in the CLI.
2. To save the installed license keys to a file or URL, enter the following command:

   request system license save *filename* | *url*

   For example, the following command saves the installed license keys to a file named license.config:

   request system license save ftp://user@host/license.conf

3. Go on to "Verifying J-series License Management" on page 11.

Verifying J-series License Management

To verify J-series license management, perform these tasks:

- Displaying Installed Licenses on page 11
- Displaying License Usage on page 12
- Displaying Installed License Keys on page 13

Displaying Installed Licenses

Purpose Verify that the expected licenses are installed and active on the Services Router.

Action From the CLI, enter the show system license command.

Sample Output

```
user@router> show system license

License usage:
                    Free ports    Licenses     Licenses    Licenses
  Feature name            used        used    installed      needed
  all                                    0            1           0
  firewall                               1            1           0
  if-t1-4                    1           1            4           0
  if-fe                      2           0            0           0
  ipsec-vpn                              1            1           0

Licenses installed:
License identifier: li29183743
  State: valid
  License version: 2
  Valid for device: jp47859620

License identifier: li48293123
```

```
  State: valid
  License version: 2
  Valid for device: jp47859620
  Features:
    firewall         - Stateful firewall

License identifier: li72194673
  State: valid
  License version: 2
  Valid for device: jp47859620
  Features:
    if-t1-4          - Four additional T1 ports

License identifier: li41597793
  State: valid
  License version: 2
  Valid for device: jp47859620
  Features:
    ipsec-vpn        - IPSec VPN tunnelling
```

What It Means The output shows a list of the license usage and a list of the licenses installed on the Services Router. Verify the following information:

- Each license is present. Licenses are listed in ascending alphanumeric order by license ID.
- The state of each license is valid.

  A state of invalid indicates that the license key is not a valid license key. Either it was entered incorrectly or it is not valid for the specific device.
- The feature for each license is the expected feature. The features enabled are listed by license. An all-inclusive license has All features listed.
- All configured features have the required licenses installed. The Licenses needed column must show that no licenses are required.

Displaying License Usage

Purpose Verify that the licenses fully cover the feature configuration on the Services Router.

Action From the CLI, enter the show system license usage command.

Sample Output

```
user@router> show system license usage

                  Free ports    Licenses     Licenses    Licenses
  Feature name           used        used    installed      needed
  all                               0           1           0
  bgp-reflection                    0           1           1
  firewall                          1           1           0
  if-t1-4                  1        3           4           0
  if-fe                    2        0           2           1
  ipsec-vpn                         2           1           1
```

What It Means The output shows a list of the licenses installed on the Services Router and how they are used. Verify the following information:

- Each licensed feature and port is present. Features and ports are listed in ascending alphabetical order by license name. The number of licenses is shown in the fourth column. Verify that the appropriate number of licenses is installed.
- The number of used licenses matches the number of configured features and ports. If a licensed feature or port is configured, the feature or port is considered used. The sample output shows that stateful firewall and BGP route reflection are configured. Additionally, four T1 interfaces (one free port and three licensed ports) are configured. Two free and two licensed Fast Ethernet ports are configured, and one Fast Ethernet license has been installed.
- A license is installed on the Services Router for each configured feature and port. For every feature or port configured that does not have a license, one license is needed.

  For example, the sample output shows that the user has configured four Fast Ethernet interfaces (two licensed interfaces and two free interfaces). This configuration requires two purchased licenses, but only one has been purchased. An additional license is required to be in compliance with license agreements.

Displaying Installed License Keys

Purpose Verify the license keys installed on the Services Router.

Action From the CLI, enter the show system license keys command.

Sample Output

```
user@router> show system license keys


li29183743 jzsn4q ix8i8d 4ky27y jzsn4q ix8i8d adj7kr
           8uq38t 82fsj6 ii8i7e adj7kr 82fsj6 acasck
           ix8i8d 4ky27y acasck 8uq38t ks2923 a938

li48293123 4ky27y acasck 82fsj6 jzsn4q ix8i8d eksi2r
           8uq38t ix8i8d jzsn4q ix8i8d 4ky27y acasck
           82fsj6 ii8i7e adj7kr 8uq38t ks2923 a9382e

li83474929 dkdis8 adj7kr 4ky27y aclsck 82fsj6 jzsn4q
           8uq38t jzsn4q 9dk2i2 ii3i8d akd239 ks2923
           492idf oo8i7e adj7kr 8u3892 3ksio
```

What It Means The output shows a list of the license keys installed on the Services Router. Verify that each expected license key is present.

Chapter 2

Managing Users and Operations

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

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

System Management Terms

Before performing system management tasks, become familiar with the terms defined in Table 9.

Table 9: 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.

System Management Overview

This section contains the following topics:

System 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 Users with Quick Configuration" on page 21 and "Managing Users and Files with a Configuration Editor" on page 34. 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 *J-series Services Router Getting Started Guide*. 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 11.

- 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 17.

- Commands and statements that users can and cannot specify. For more information, see "Denying or Allowing Individual Commands" on page 19.

- 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 11. 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 10).

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 10: Permission Bits for Login Classes

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

Permission Bit	Access
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 11: 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 41.

System Log Files

The JUNOS software generates system log messages (also called syslog 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.

When you configure system logging, you can direct messages to one or more destinations:

- To a named file in a local file system
- To the terminal session of one or more specific users (or all users) when they are logged into the router
- To the router console
- To a remote machine that is running the UNIX syslogd utility

Each system log message belongs to a facility, which is a group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts).

Reboot requests are recorded to the system log files, which you can view with the show log command. Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the show system processes command.

Before You Begin

Before you perform any system management tasks, you must perform the initial Services Router configuration described in the *J-series Services Router Getting Started Guide*.

Managing Users and Files with the J-Web Interface

This section contains the following topics:

Managing Users with Quick Configuration

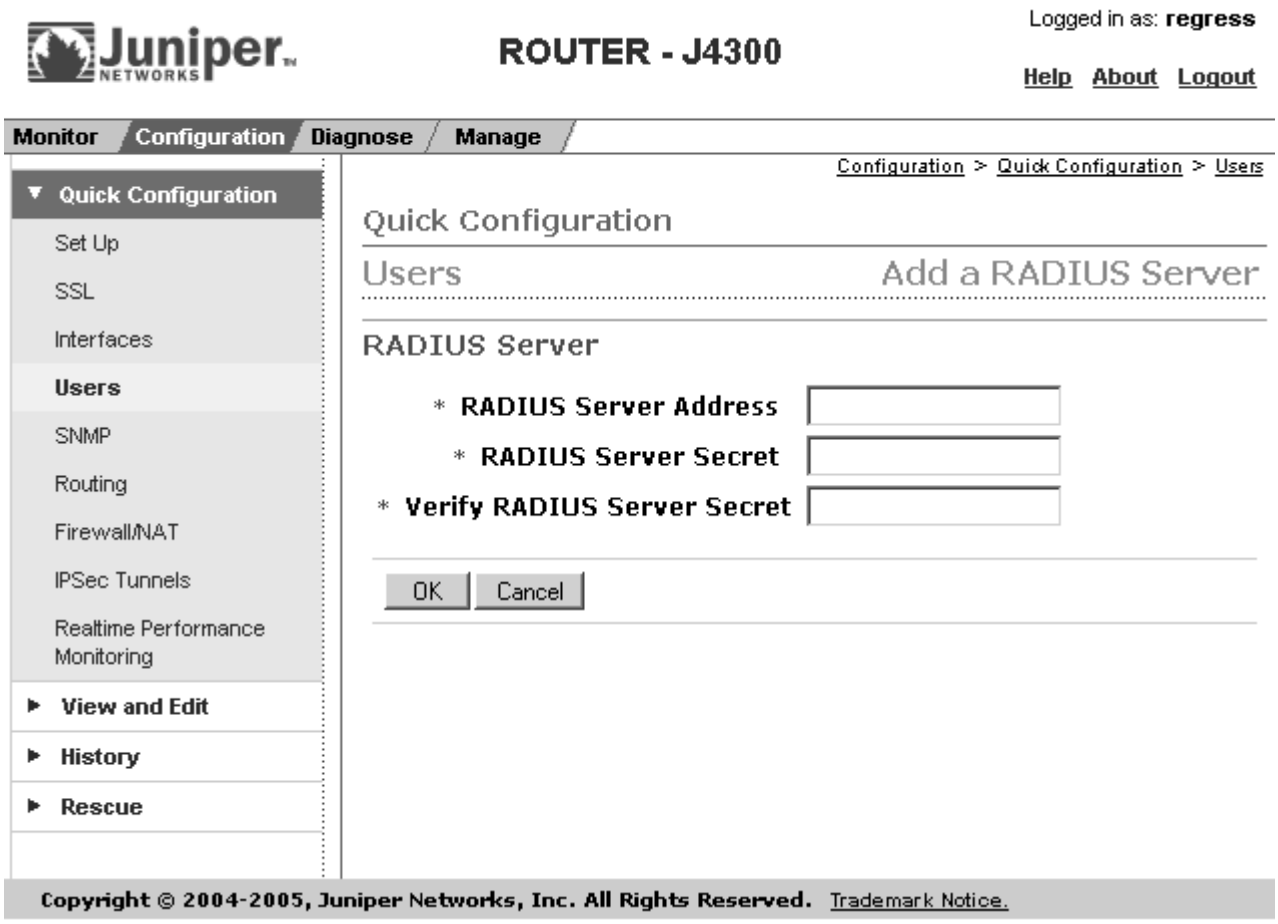
This section contains the following topics:

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 2 shows the Users Quick Configuration page for RADIUS servers.

Figure 2: 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 12.
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 12: Users Quick Configuration for RADIUS Servers Summary

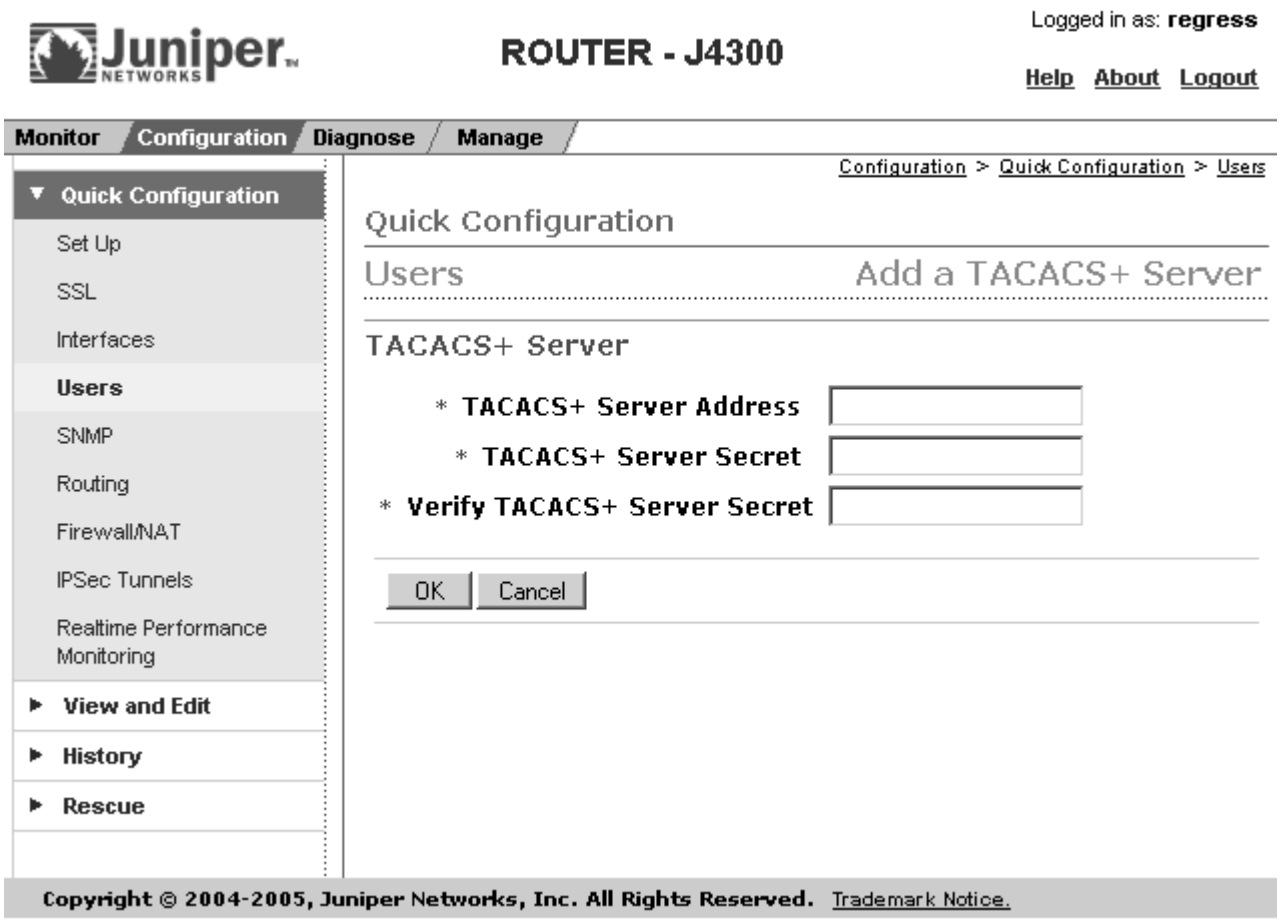
Field	Function	Your Action
RADIUS Server		
RADIUS Server Address (required)	Identifies the IP address of the RADIUS server.	Type the RADIUS server's 32-bit IP address, in dotted decimal notation.
RADIUS Server Secret (required)	The secret (password) of the RADIUS server.	Type the secret (password) of 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 3 shows the Users Quick Configuration page for TACACS+ servers.

Figure 3: 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 13.
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 13: Users Quick Configuration for TACACS+ Servers Summary

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

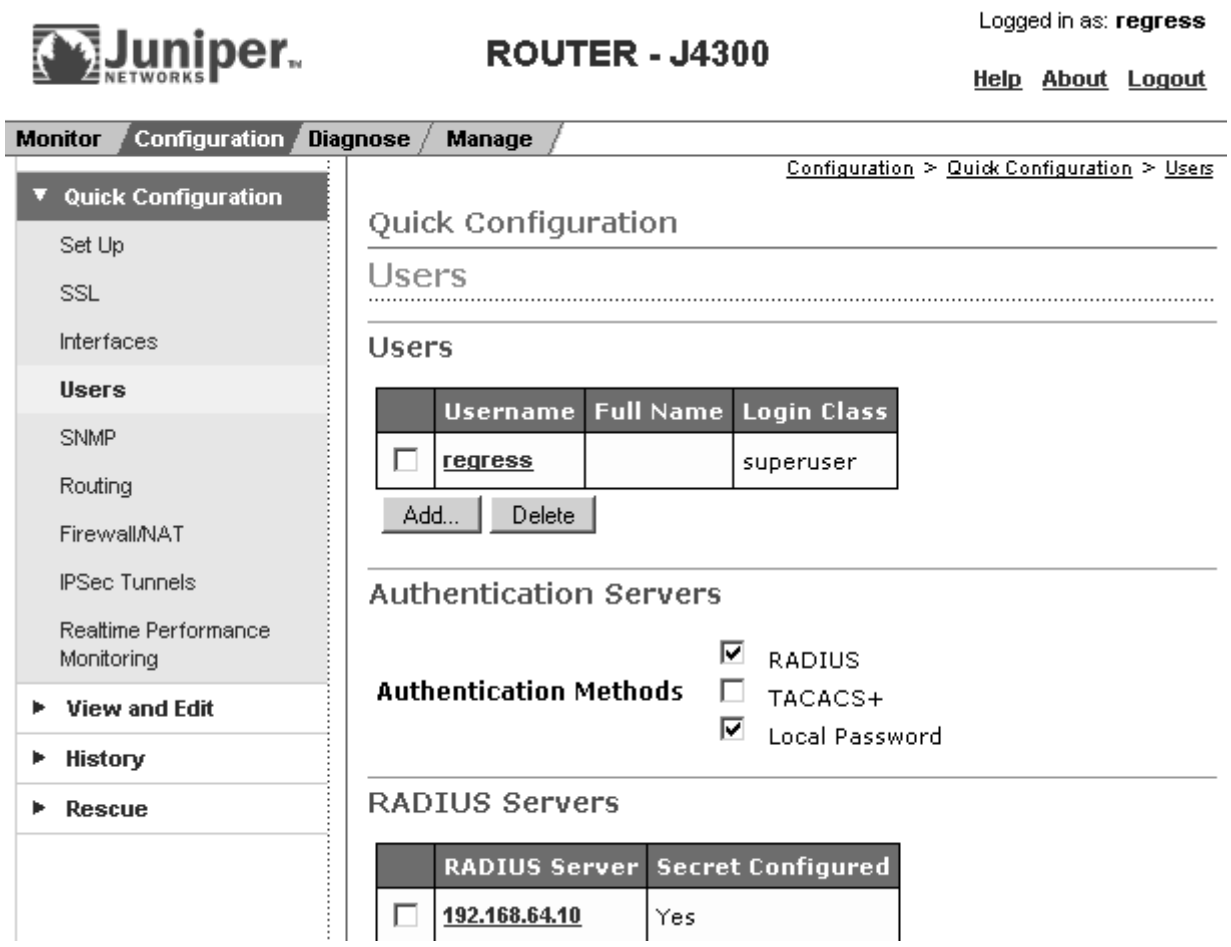
Configuring System Authentication

On the Users Quick Configuration page, you can configure the authentication methods the Services Router uses to verify that a user can gain access. For each login attempt, the router tries the authentication methods in order, starting with the first one, until the password matches.

If you do not configure system authentication, users are verified based on their configured local passwords.

Figure 4 shows the Users Quick Configuration page.

Figure 4: 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**.

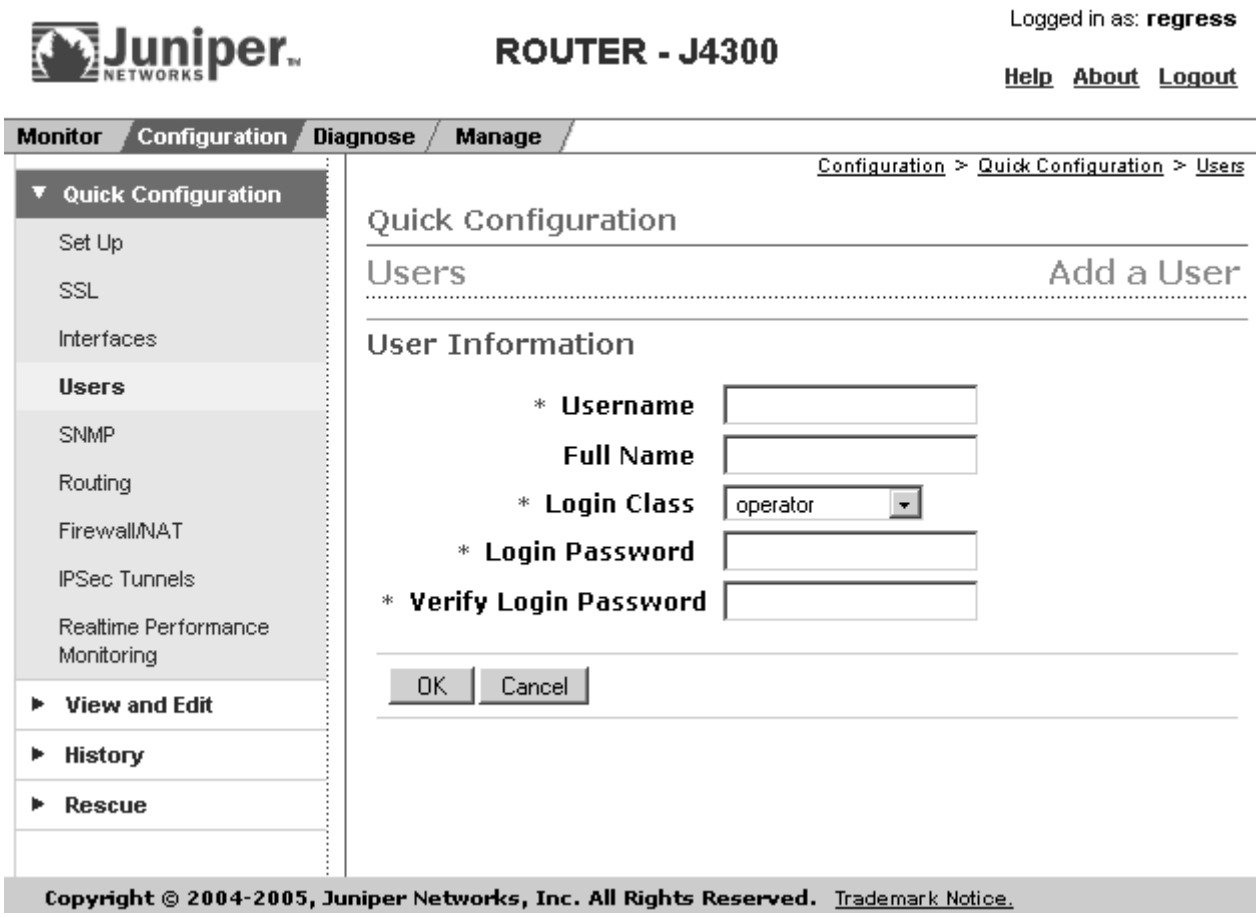
- To apply the configuration and return to the Quick Configuration page, click **OK**.
- To cancel your entries and return to the Quick Configuration page, click **Cancel**.

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 5 shows the Quick Configuration page for adding a user.

Figure 5: 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 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 14: 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 drop-down 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 17.

Field	Function	Your Action
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 Files with the J-Web Interface

This section contains the following topics:

Cleaning Up Files

You can use the J-Web interface to rotate and delete 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 6 shows the Clean Up Files page.

Figure 6: Clean Up Files Page

To rotate and delete 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**.

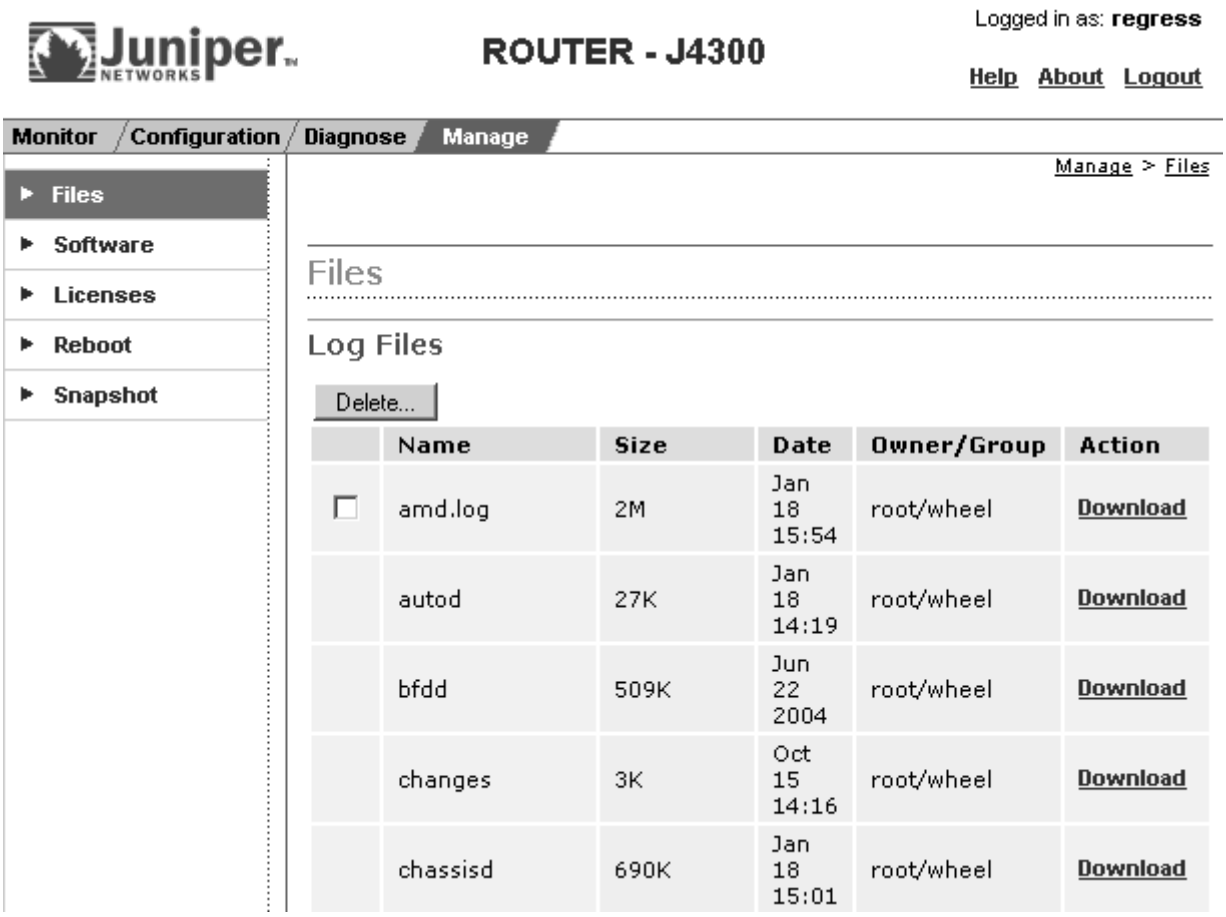
- To cancel your entries and return to the list of files in the directory, click **Cancel**.

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 7 shows the J-Web page from which you can download log files.

Figure 7: 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.

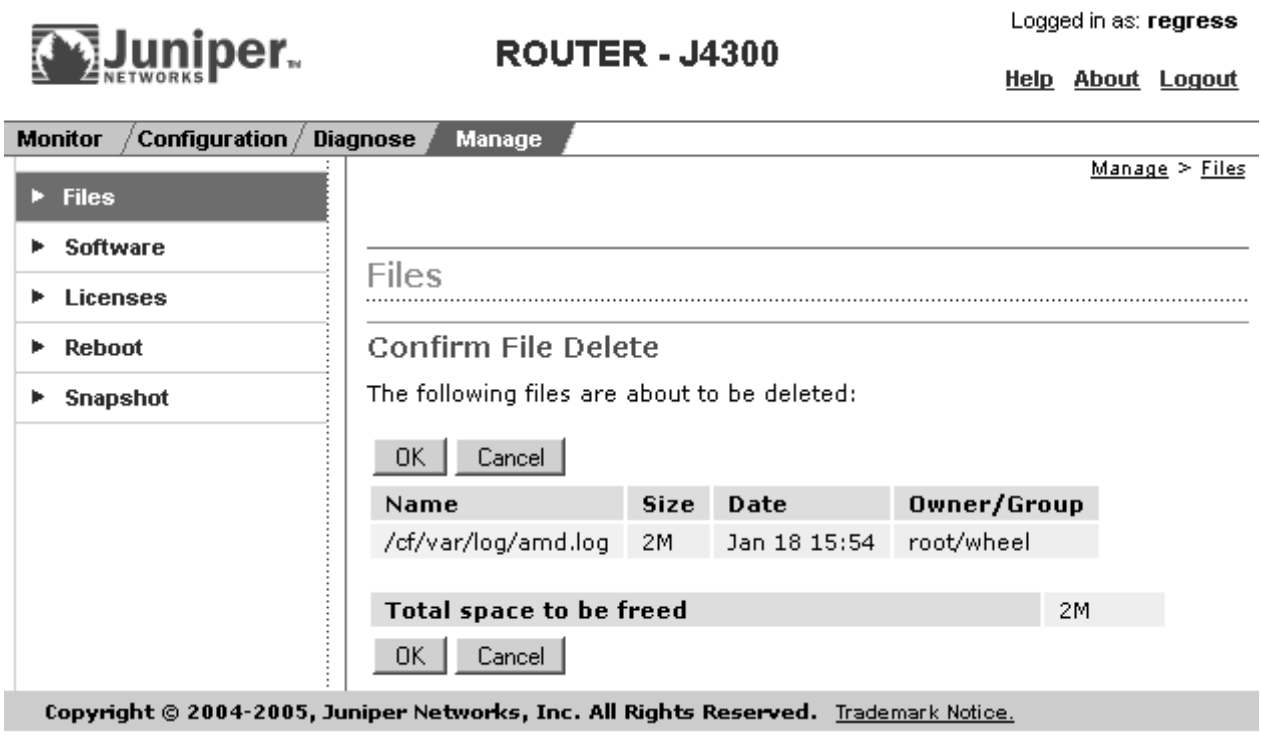
Deleting Files

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

Figure 8 shows the J-Web page on which you confirm the deletion of files.

Figure 8: Confirm File Delete Page



To rotate and 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**.

Managing Users and Files with a Configuration Editor

This section contains the following topics:

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 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 37.
- To configure a remote user template account, see “Creating a Remote Template Account” on page 41.
- To configure local user template accounts, see “Creating a Local Template Account” on page 42.

Table 15: Setting Up RADIUS Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System**.	From the top of the configuration hierarchy enter edit system
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 16.
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 37.
   - To configure a remote user template account, see "Creating a Remote Template Account" on page 41.
   - To configure local user template accounts, see "Creating a Local Template Account" on page 42.

Table 16: Setting Up TACACS+ Authentication

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System**.	From the top of the configuration hierarchy 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 17.
3. If you are finished configuring the network, commit the configuration.

   To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and 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 34.
   - To configure a TACACS+ server, see "Setting Up TACACS+ Authentication" on page 35.
   - To configure a remote user template account, see "Creating a Remote Template Account" on page 41.
   - To configure local user template accounts, see "Creating a Local Template Account" on page 42.

Table 17: Configuring Authentication Order

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System**.	From the top of the configuration hierarchy enter edit system
Add RADIUS authentication to the authentication order.	1. In the Authentication order box, click **Add new entry**. 2. In the drop-down 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 drop-down 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

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 40 and "Setting Up Template Accounts" on page 41.

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 17.

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 18.
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 40.
   - To create shared user accounts, see "Setting Up Template Accounts" on page 41.

Table 18: Defining Login Classes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Login** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Login**.	From the top of the configuration hierarchy enter edit system login

Task	J-Web Configuration Editor	CLI Configuration Editor
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"
Give the operator-and-boot login class operator privileges.	1. Next to Permissions, click **Add new entry**. 2. In the Value drop-down list, select **clear**. 3. Click **OK**. 4. Next to Permissions, click **Add new entry**. 5. In the Value drop-down list, select **network**. 6. Click **OK**. 7. Next to Permissions, click **Add new entry**. 8. In the Value drop-down list, select **reset**. 9. Click **OK**. 10. Next to Permissions, click **Add new entry**. 11. In the Value drop-down list, select **trace**. 12. Click **OK**. 13. Next to Permissions, click **Add new entry**. 14. In the Value drop-down 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 34 and "Setting Up TACACS+ Authentication" on page 35.)

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 19.
3. If you are finished configuring the network, commit the configuration.

Table 19: Creating User Accounts

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Login** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Login**.	From the top of the configuration hierarchy 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 20.
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 34.
   - To configure a TACACS+ server, see "Setting Up TACACS+ Authentication" on page 35.
   - To specify a system authentication order, see "Configuring Authentication Order" on page 37.

Table 20: Creating a Remote Template Account

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Login** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Login**.	From the top of the configuration hierarchy 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 21.
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 34.
   - To configure a TACACS+ server, see “Setting Up TACACS+ Authentication” on page 35.
   - To configure a system authentication order, see “Configuring Authentication Order” on page 37.

Table 21: Creating a Local Template Account

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Login** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Login**.	From the top of the configuration hierarchy 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

Using System Logs

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.

For each place where you can send system logging information, you specify the class (facility) of messages to log and the minimum severity level (level) of the message.

Table 22 lists the system logging facilities, and Table 23 lists the system logging severity levels. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Table 22: System Logging Facilities

Facility	Description
any	Any facility
authorization	Any authorization attempt
change-log	Any change to the configuration
cron	Cron scheduling process
daemon	Various system processes
interactive-commands	Commands executed in the CLI
kernel	Messages generated by the JUNOS kernel
user	Messages from random user processes

Table 23: System Logging Severity Levels

Severity Level (from Highest to Lowest Severity)	Description
emergency	Panic or other conditions that cause the system to become unusable.
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.
warning	System warning messages.
notice	Conditions that are not error conditions, but that might warrant special handling.
info	Informational messages. This is the default.
debug	Software debugging messages.

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 drive. The default directory for log files is /var/log. To specify a different directory on the compact flash drive, include the complete pathname. For the list of logging facilities and severity levels, see Table 22 and Table 23.

For information about archiving log files, see “Archiving System Logs” on page 46.

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 24.
3. If you are finished configuring the network, commit the configuration.

Table 24: Sending Messages to a File

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Syslog** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Syslog**.	From the top of the configuration hierarchy 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 drop-down menu, select **authorization**. 5. In the Level drop-down menu, 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 22 and Table 23.

The procedure provided in this section sends send 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 25.
3. If you are finished configuring the network, commit the configuration.

Table 25: Sending Messages to a User Terminal

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System Syslog** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Syslog**.	From the top of the configuration hierarchy 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 drop-down menu, select **any**. 5. In the Level drop-down menu, 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*.

Accessing Remote Devices with the CLI

This section contains the following topics:

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 26 describes the telnet command options. For more information, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

Table 26: 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> <logical-router logical-router-name>
<routing-instance routing-instance-name> <source address> <v1> <v2>
```

Table 27 describes the ssh command options. For more information, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

Table 27: CLI ssh Command Options

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

Chapter 3

Configuring SNMP for Network Management

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

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

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

Network Management Overview

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

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

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

Managers and Agents

Because SNMP is a client/server protocol, SNMP nodes can be classified as either clients (SNMP managers) or servers (SNMP agents).

SNMP managers, also called network management systems (NMSs), occupy central points in the network and they actively query and collect messages from SNMP agents in the network. SNMP agents are individual processes running on network nodes that gather information for a particular node and transfer the information to SNMP managers as queries are processed. Because SNMP agents are individual SNMP processes running on a host, multiple agents can be active on a single network node at any given time.

SMI, MIBs, and OIDs

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

Standard and Enterprise MIBs

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

SNMP Requests

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

SNMP Communities

To help ensure that only specific SNMP managers can access a particular SNMP agent, SNMP access is granted through communities. To control access, you first create an SNMP community. The community is assigned a name that is unique on the host. All SNMP requests that are sent to the agent must be configured with the same community name.

When multiple agents are configured on a particular host, the community name process ensures that SNMP requests are sorted to only those agents configured to handle the requests.

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

SNMP Traps

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

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

Before You Begin

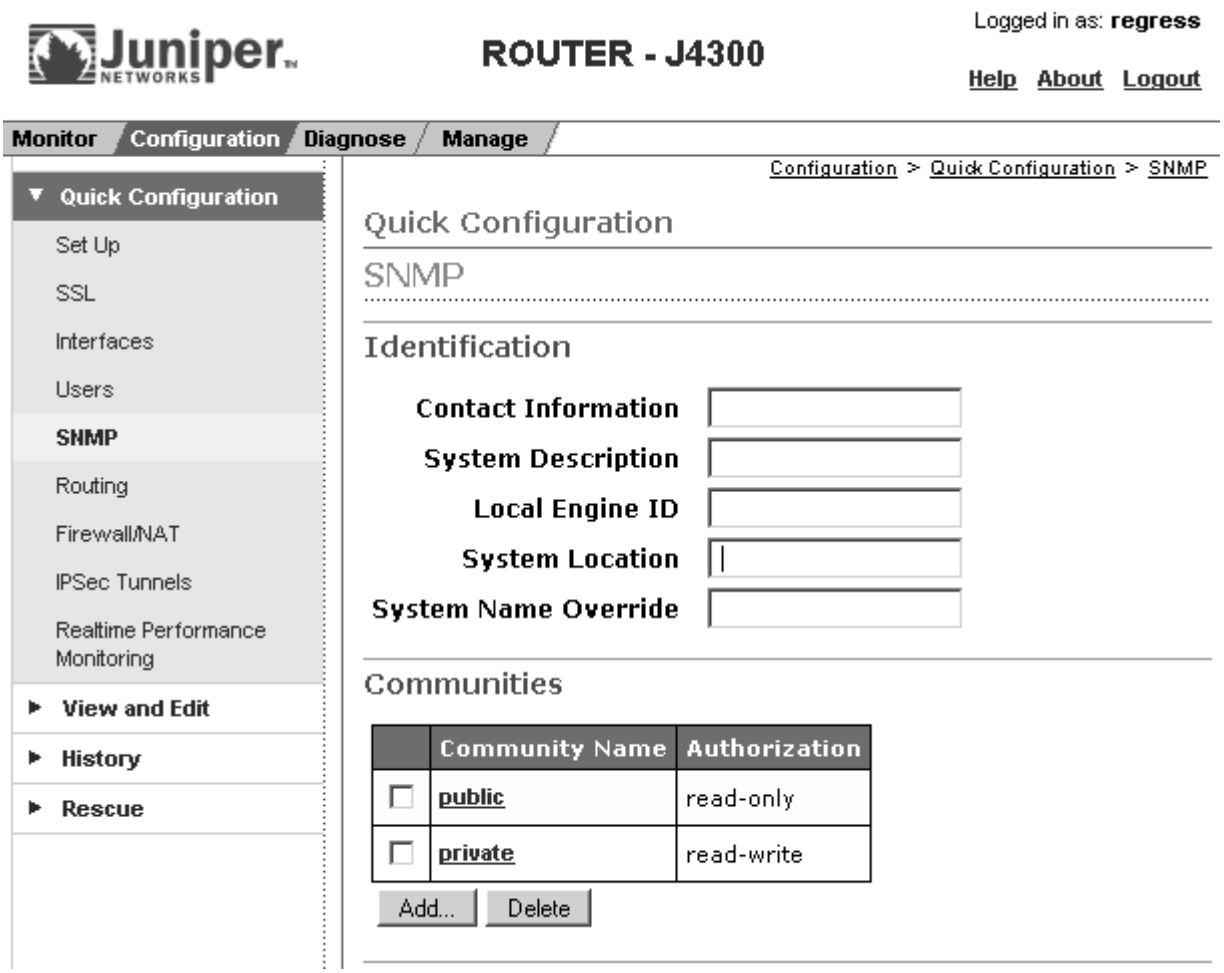
Before you begin configuring SNMP, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See the *J-series Services Router Configuration Guide*.

Configuring SNMP with Quick Configuration

J-Web Quick Configuration allows you to define system identification information, create SNMP communities, and create SNMP trap groups. Figure 9 shows the Quick Configuration page for SNMP.

Figure 9: 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 28.
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 59.

Table 28: 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 fe-0/0/0.	Type the MAC address of the fe-0/0/0 interface.
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 defined in the *J-series Services Router Getting Started Guide*.	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 drop-down menu.
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.

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**.

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 Configuration Guide*.

■ Defining System Identification Information (Required) on page 55

■ Configuring SNMP Agents and Communities (Required) on page 56

- Managing SNMP Trap Groups (Required) on page 57
- Controlling Access to MIBs (Optional) on page 58

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

Table 29: System Identification Information and Corresponding MIBs

System Information	MIB
Contact	sysContact
System location	sysLocation
System description	sysDescription
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 30.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 59.

Table 30: Configuring Basic System Identification

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	In the configuration editor hierarchy, select **Snmp**.	From the top of the configuration hierarchy, enter edit snmp
Configure the system contact information (such as a name and phone number).	In the Contact box, type the contact information as a free-form text string.	Set the contact information: set contact "*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*"

Task	J-Web Configuration Editor	CLI Configuration Editor
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 *J-series Services Router Getting Started Guide*.	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 fe-0/0/0 as the engine ID suffix.	1. Select **Engine id**. 2. In the Engine id choice box, select **Use mac address** from the drop-down menu. 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 31.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 59.

Table 31: Configuring SNMP Agents and Communities

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	In the configuration editor hierarchy, select **Snmp**.	From the top of the configuration hierarchy, enter edit snmp

Task	J-Web Configuration Editor	CLI Configuration Editor
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 drop-down menu.	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 32.
3. If you are finished configuring the network, commit the configuration.

4. To check the configuration, see "Verifying the SNMP Configuration" on page 59.

Table 32: Configuring SNMP Trap Groups

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	In the configuration editor hierarchy, select **Snmp**.	From the top of the configuration hierarchy, 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* target 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 33.
3. If you are finished configuring the network, commit the configuration.
4. To check the configuration, see "Verifying the SNMP Configuration" on page 59.

Table 33: Configuring SNMP Views

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **SNMP** level in the configuration hierarchy.	In the configuration editor hierarchy, select **Snmp**.	From the top of the configuration hierarchy, 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 drop-down menu, 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 drop-down menu, 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.

Sample Output

```
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.

For more information about show snmp statistics, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

Chapter 4

Configuring the 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 the J-Web configuration editor or CLI configuration editor to configure the DHCP server.

This chapter contains the following topics:

DHCP Terms

Before configuring the DHCP server on J-series Services Routers, become familiar with the terms defined in Table 34.

Table 34: 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

You can also configure the Services Router to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Services Router).
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

Compatibility with Autoinstallation

Services Router DHCP server functions are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Conflict Detection and Resolution

A client that receives an IP address from the Services Router operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The Services Router maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the show system services dhcp conflicts command. The addresses in the conflicts list remain excluded until you use the clear system services dhcp conflict command to manually clear the list.

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 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 35 provides the settings and values for the sample DHCP server configuration used in this section.

Table 35: Sample DHCP Server Configuration Settings

Settings	Sample Value or Values
DHCP Subnet Configuration	
Address pool subnet address	192.168.2.0/24
High address in the pool range	192.168.2.254
Low address in the pool range	192.168.2.2
Address pool default lease time, in seconds	1,209,600 (14 days)
Address pool maximum lease time, in seconds	2,419,200 (28 days)

Settings	Sample Value or Values
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 36.
3. If you are finished configuring the network, commit the configuration.
4. To verify DHCP server configuration and operation, see "Verifying a DHCP Server Configuration" on page 67.

Table 36: Configuring the DHCP Server

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Dhcp server** level in the configuration hierarchy.	In the configuration editor hierarchy, select **System > Services > Dhcp server**.	From the top of the configuration hierarchy, enter edit system services dhcp-server
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

Task	J-Web Configuration Editor	CLI Configuration Editor
Define the default and maximum lease times, in seconds.	1. From the Default lease time drop-down list, select **Enter Specific Value**. 2. In the Length box, type 1209600. 3. From the Maximum lease time drop-down 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
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 drop-down 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

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-server command from the top level.

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

Sample Output

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

What It Means Verify that the output shows the intended configuration of the DHCP server. For more information about the format of a configuration file, see the *J-series Services Router 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 64 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.

Sample Output

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

IP Address   Hardware Address   Binding Type  Lease Expires
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

DHCP binding information:
    IP address          192.168.2.2
    Hardware address    02:04:06:08:0A:0C
    Pool                192.168.2.0/24
    Interface           fe-0/0/0

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

DHCP options:
    name-server 192.168.10.2
    domain-name mycompany.net mylab.net
    option 16 Ip address 192.168.2.33

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

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 conflicts command does not display any conflicts.

Verifying DHCP Server Operation

Purpose Verify that the DHCP server is operating as configured.

Action Take the following actions:

- Use the ping command to verify that a client responds to ping packets containing the destination IP address assigned by the Services Router.
- Display the IP configuration on the client. For example, on a PC running Microsoft Windows, enter ipconfig /all at the command prompt to display the PC's IP configuration.

Sample Output

```
user@host> ping 192.168.2.2

PING 192.168.2.2 (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: icmp_seq=0 ttl=255 time=8.856 ms
64 bytes from 192.168.2.2: icmp_seq=1 ttl=255 time=11.543 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=255 time=10.315 ms
...

C:\Documents and Settings\user> ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : my-pc
        Primary DNS Suffix  . . . . . . . : mycompany.net
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : mycompany.net
                                            mylab.net

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : mycompany.net mylab.net
        Description . . . . . . . . . . . : 10/100 LAN Fast Ethernet Card
        Physical Address. . . . . . . . . : 02-04-06-08-0A-0C
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
```

```
IP Address. . . . . . . . . . . . : 192.168.2.2
Subnet Mask . . . . . . . . . . . : 255.255.254.0
Default Gateway . . . . . . . . . : 192.168.10.3
DHCP Server . . . . . . . . . . . : 192.168.2.1
DNS Servers . . . . . . . . . . . : 192.168.10.2
Primary WINS Server . . . . . . . : 192.168.10.4
Secondary WINS Server . . . . . . : 192.168.10.5
Lease Obtained. . . . . . . . . . : Monday, January 24, 2005 8:48:59 AM
Lease Expires . . . . . . . . . . : Monday, February 7, 2005 8:48:59 AM
```

What It Means Verify the following:

- The client returns a ping response.

  For information about using the J-Web interface to ping a host, see "Using the J-Web Ping Host Tool" on page 112. For more information about the ping command, see "Using the ping Command" on page 126 or the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

- The client IP configuration displayed contains the configured values. For example, for the DHCP configuration in "Configuring the DHCP Server with a Configuration Editor" on page 64, you can verify the following settings:

  - DNS Suffix Search List is correct.
  - IP address is within the IP address pool you configured.
  - DHCP Server is the primary IP address of the Services Router interface on which the DHCP message exchange occurs. If you include the server-identifier statement in your configuration, the DHCP server IP address specified in this statement is displayed.
  - Lease Obtained and Lease Expires times are correct.

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

Displaying DHCP Statistics

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

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

Sample Output

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

Default settings:
    Default lease time        14 days
    Minimum lease time         1 minute
    Maximum lease time        28 days
    BOOTP lease length         0 seconds
    BOOTP lease cutoff         unknown
```

```
Packets dropped:
    Total                     0
    Bad hardware address      0
    Bad opcode                0
    Invalid server address    0
    No available addresses    0
    No interface match        0
    No routing instance match 0
    No valid local address    0
    Packet too short          0
    Read error                0
    Send error                0

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

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

What It Means Verify the following:

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

Chapter 5

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 37.

Table 37: 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.

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. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web or CLI display.

Alarm Severity

Alarms on a Services Router have two severity levels:

- Major (red)—Indicates a critical situation on the router that has resulted from one of the following conditions. A red alarm condition requires immediate action.
  - One or more hardware components have failed.
  - One or more hardware components have exceeded temperature thresholds.
  - An alarm condition configured on an interface has triggered a critical warning.
- Minor (yellow)—Indicates a noncritical condition on the router that, if left unchecked, might cause an interruption in service or degradation in performance. A yellow alarm condition requires monitoring or maintenance.

  A missing rescue configuration or software license generates a yellow system alarm.

Alarm Conditions

To enable alarms on a Services Router interface, you must select an alarm condition and an alarm severity. In contrast, alarm conditions and severity are preconfigured for chassis alarms and system alarms.

This section contains the following topics:

- Interface Alarm Conditions on page 75
- Chassis Alarm Conditions and Corrective Actions on page 78
- System Alarm Conditions and Corrective Actions on page 79

Interface Alarm Conditions

Table 38 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 38: Interface Alarm Conditions

Interface	Alarm Condition	Description	Configuration Option
DS1 (T1)	Alarm indication signal	The normal T1 traffic signal contained a defect condition and has been replaced by the AIS. A transmission interruption occurred at the remote endpoint or upstream of the remote endpoint. This all-ones signal is transmitted to prevent consequential downstream failures or alarms.	ais
	Yellow alarm	The remote endpoint is in red alarm failure. This condition is also known as a far end alarm failure.	ylw
Ethernet (Fast Ethernet)	Link is down	The physical link is unavailable.	link-down
Integrated services	Hardware or software failure	On the adaptive services module, either the hardware associated with the module, or the software that drives the module, has failed.	failure
Serial	Clear-to-Send signal absent	The remote endpoint of the serial link is not transmitting a CTS signal. The CTS signal must be present before data can be transmitted across a serial link.	cts-absent
	Data Carrier Detect signal absent	The remote endpoint of the serial link is not transmitting a DCD signal. Because the DCD signal transmits the state of the router, no signal probably indicates that the remote endpoint of the serial link is unavailable.	dcd-absent
	Data Set Ready signal absent	The remote endpoint of the serial link is not transmitting a DSR signal. The DSR signal indicates that the remote endpoint is ready to receive and transmit data across the serial link.	dsr-absent
	Loss of receive clock	The clock signal from the remote endpoint is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-rx-clock
	Loss of transmit clock	The local clock signal is not present. Serial connections require clock signals to be transmitted from one endpoint and received by the other endpoint of the link.	loss-of-tx-clock

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
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 39 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 39: Chassis Alarm Conditions and Corrective Actions

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

System Alarm Conditions and Corrective Actions

Table 40 lists the two preset system alarms, the condition that triggers each alarm, and the action you take to correct the condition.

Table 40: 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 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 "Installing and Managing J-series Licenses" on page 3.

Before You Begin

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

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See the *J-series Services Router 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 75.

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 41.
3. If you are finished configuring the network, commit the configuration.
4. To verify the alarms configuration, see "Displaying Alarm Configurations" on page 83.

5. To check the status of active alarms, see “Checking Active Alarms” on page 81.

Table 41: Configuring Interface Alarms

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Alarm** level in the configuration hierarchy.	In the configuration editor hierarchy, select **Chassis > Alarm**.	From the top of the configuration hierarchy, 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 drop-down list, select **red**. 3. Click **OK**.	Enter set ds1 ylw red
Configure the system to generate a red interface alarm when a link down failure is detected on a Fast Ethernet link.	1. In the Ethernet field, click **Configure**. 2. From the Link down drop-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 drop-down list, select **yellow**. 3. From the Dcd absent drop-down list, select **yellow**. 4. From the Loss of rx clock drop-down list, select **red**. 5. From the Loss of tx clock drop-down 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

Task	J-Web Configuration Editor	CLI Configuration Editor
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 drop-down list, select **red**. 3. From the Exz drop-down list, select **yellow**. 4. From the Los drop-down list, select **red**. 5. Click **OK**.	1. Enter set t3 ylw red 2. Enter set t3 exz yellow 3. Enter set t3 los red
Configure the system to display active system alarms whenever a user with the login class admin logs in to the router.	1. From the top of the configuration editor hierarchy, select **System > Login**. 2. In the Class field, click **Add new entry**. 3. In the Class name field, type admin. 4. Select the **Login alarms** check box. 5. Click **OK**. 6. Add the login class admin to users. For details, see "Defining Login Classes" on page 38.	1. Enter edit system login 2. Enter set class admin login-alarms 3. Add the login class admin to users. For details, see "Defining Login Classes" on page 38.

Checking Active Alarms

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

- show chassis alarms
- show system alarms

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

Figure 10 shows the View Alarms summary page. Click an alarm in the list of active alarms to display a detailed alarm message.

Figure 10: J-Web View Alarms Summary Page

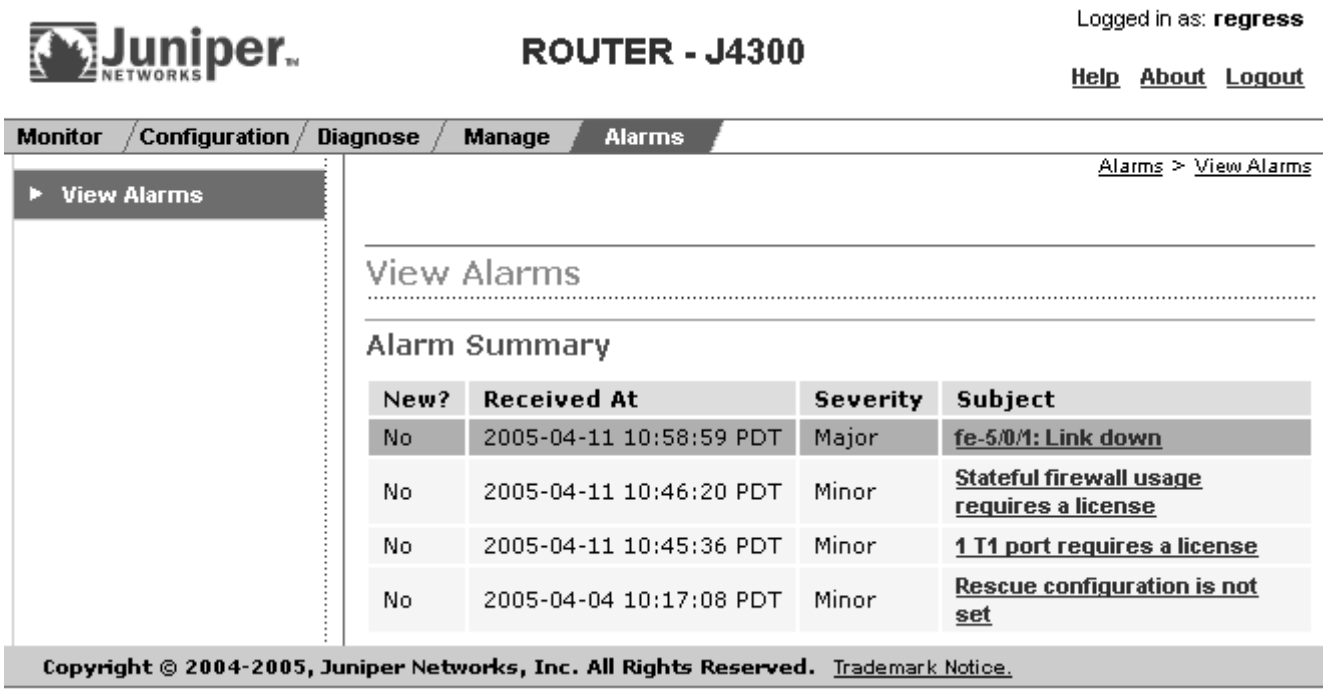


Table 42 summarizes the output fields on the alarms page.

Table 42: 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.	

Field	Values	Additional Information
Severity	Alarm severity—either major (red) or minor (yellow).	A major (red) alarm condition requires immediate action. A minor (yellow) condition requires monitoring or maintenance.
Alarm Type	Category of the alarm: ■ Chassis—Indicates an alarm condition on the chassis (typically an environmental alarm such as temperature) ■ Configuration—Indicates that no rescue configuration is set ■ ETHER—Indicates an alarm condition on a Fast Ethernet interface ■ DS3—Indicates an alarm condition on a DS3 interface ■ License—Indicates a software license infringement ■ Serial—Indicates an alarm condition on a serial interface ■ Services—Indicates an alarm condition on the services module	

Verifying the Alarms Configuration

To verify alarms configuration, perform the following task.

Displaying Alarm Configurations

Purpose Verify the configuration of the alarms.

Action From the J-Web interface, select **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the show chassis alarms command.

Sample Output

```
[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
- Fast Ethernet alarms
- Serial alarms

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

Chapter 6

Monitoring and Diagnosing a Services Router

J-series Services Routers support a suite of J-Web tools and CLI operational mode commands for monitoring and managing system health and performance. Monitoring tools and commands display the current state of the router. 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 Protocols, Class of Service, and System Basics Command Reference* and the *JUNOS Network and Services Interfaces Command Reference*.

Monitoring and Diagnostic Terms

Before monitoring and diagnosing J-series Services Routers, become familiar with the terms defined in Table 43.

Table 43: J-series Monitoring and Diagnostic 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.
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.

Term	Definition
Internet Control Message Protocol (ICMP)	TCP/IP protocol used to send error and information messages.
routing instance	Collection of routing tables, interfaces, and routing protocol interfaces. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables.
loose source routing	Option in the IP header used to route a packet based on information supplied by the source. A gateway or host must route the packet using the routers specified by this information, but the packet can use other routers along the way.
routing table	Database of routes learned from one or more protocols.
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.

Monitoring and Diagnostic Tools Overview

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

You can also monitor and 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:

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

Table 44: J-Web Monitor Options and CLI show Commands

Monitor Option	Function	Corresponding CLI Commands
System	Displays Services Router system properties, such as the system identification and uptime, users, and resource usage. For details, see "Monitoring System Properties" on page 92.	■ show system uptime ■ show system users ■ show system storage ■ show system processes
Chassis	Displays alarm, environment, and hardware information. For details, see "Monitoring the Chassis" on page 95.	■ show chassis alarms ■ show chassis environment ■ 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 96.	■ show interfaces terse ■ show interfaces detail ■ show interfaces *interface-name*
Routing	Displays routing information through the following options: ■ Route Information—Displays all routes in the routing table, including protocol, state, and parameter information. You can narrow the list of routes displayed by specifying search criteria. ■ OSPF Information—Displays a summary of OSPF neighbors, interfaces, and statistics. ■ BGP Information—Displays a summary of BGP routing and neighbor information. ■ RIP Information—Displays a summary of RIP neighbors and statistics. For details, see "Monitoring Routing Information" on page 99.	■ 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

Monitor Option	Function	Corresponding CLI Commands
Service Sets	Displays information about configured service sets. For details, see "Monitoring Service Sets" on page 103.	■ 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 104.	■ 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 106.	■ show services ipsec-vpn ipsec statistics ■ show services ipsec-vpn ike security-associations
NAT	Displays configured NAT pools. For details, see "Monitoring NAT Pools" on page 107.	■ show services nat pool

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 45 describes the functions of the Diagnose and Manage options.

Table 45: 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 112.
Ping MPLS	Allows you to ping an MPLS endpoint using various options. For details, see "Checking MPLS Connections" on page 116.
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 "Using the J-Web Traceroute Tool" on page 122.

Option	Function
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 29.
Upgrade	Allows you to upgrade and manage Services Router software packages. For details, see "Performing Software Upgrades and Reboots" on page 159.
Licenses	Displays a summary of the licenses needed and used for each feature that requires a license. Allows you to add licenses. For details, see "Managing J-series Licenses with the J-Web Interface" on page 6.
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 175.

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 *J-series Services Router Getting Started Guide*.)

At the top level of operational mode are the broad groups of CLI diagnostic commands listed in Table 46.

Table 46: 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 "Using mtrace Commands" on page 135.

Command	Function
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 129 ■ "Using the monitor traffic Command" on page 131 ■ "Using the monitor file Command" on page 135
ping	Determines the reachability of a remote network host. For details, see "Using the ping Command" on page 126.
ping mpls	Determines the reachability of an MPLS endpoint using various options. For details, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.
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 "Using the traceroute Command" on page 128.
Connecting to Other Network Systems	
ssh	Opens secure shell connections. For details, see "Using the ssh Command" on page 47.
telnet	Opens telnet sessions to other hosts on the network. For details, see "Using the telnet Command" on page 47.
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.
start	Exits the CLI and starts a UNIX shell.
configuration	Enters configuration mode. For details, see the *J-series Services Router Getting Started Guide*.
quit	Exits the CLI and returns to the UNIX shell.

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 System Basics Configuration 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 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 27 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
- show system processes

Table 47 summarizes key output fields in system properties displays.

Table 47: Summary of Key System Properties Output Fields

Field	Values	Additional Information
System Identification		
Serial Number	Serial number for the J-series Services Router.	
JUNOS Software Version	Version of JUNOS software active on the Services Router.	
Router Hostname	Hostname of the Services Router, as defined with the set system hostname command.	

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

Field	Values	Additional Information
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.	
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.

Field	Values	Additional Information
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 the Chassis

The chassis properties include the status of any alarms on the Services Router, environment measurements, and a summary of the field-replaceable units (FRUs) on the router. To view these chassis properties, select **Monitor > Chassis** in the J-Web interface, or enter the following CLI show commands:

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

Table 48 summarizes key output fields in chassis displays.

Table 48: Summary of Key Chassis Output Fields

Field	Values	Additional Information
Alarm Summary		
Alarm Time	Date and time alarm was first recorded.	
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 73.
Alarm Description	A brief synopsis of the alarm.	
Environment Information		

Field	Values	Additional Information
Name	Chassis component. For J-series Services Routers, the chassis components are the Routing Engine, flexible PIM concentrator (FPC), and physical interface module (PIM)—identified in the display as a PIC.	On Services Routers, an FPC and a PIM are the same physical unit.
Gauge Status	Status of the temperature gauge on the specified hardware component.	
Temperature	Temperature of the air flowing past the hardware component.	
Hardware Summary		
Name	Chassis component. For J-series Services Routers, the chassis components are the Routing Engine, FPC, and PIM—identified in the display as a PIC.	On Services Routers, an FPC and a PIM are the same physical unit.
Version	Revision level of the specified hardware component.	Supply the version number when reporting any hardware problems to customer support.
Part Number	Part number of the chassis component.	
Serial Number	Serial number of the chassis component. The serial number of the backplane is also the serial number of the router chassis.	Use this serial number when you need to contact customer support about the router chassis.
Description	Brief description of the hardware item.	For PIMs, the description lists the number and type of the ports on the PIM—identified in the display as a PIC.

Monitoring the Interfaces

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

Alternatively, enter the following CLI show commands:

- show interfaces terse
- show interfaces detail
- show interfaces *interface-name*

Table 49 summarizes key output fields in interfaces displays.

Table 49: Summary of Key Interfaces Output Fields

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

Field	Values	Additional Information
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

Routing information is divided into multiple parts:

- To view the inet.0 (IPv4) routing table in the J-Web interface, select **Monitor > Routing > Route Information**, or enter the following CLI commands:
  - show route terse
  - show route detail
- To view BGP routing information, select **Monitor > Routing > BGP Information**, or enter the following CLI commands:
  - show bgp summary
  - show bgp neighbor
- 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
- To view RIP routing information, select **Monitor > Routing > RIP Information**, or enter the following CLI commands:
  - show rip statistics
  - show rip neighbors

Table 50 summarizes key output fields in routing displays.

Table 50: Summary of Key Routing Output Fields

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

Field	Values	Additional Information
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.
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 the Ethernet management port 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 Protocols, Class of Service, and System Basics 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.	
BGP Summary		
Groups	Number of BGP groups.	
Peers	Number of BGP peers.	
Down Peers	Number of unavailable BGP peers.	
Peer	Address of each BGP peer.	
InPkt	Number of packets received from the peer,	

Field	Values	Additional Information
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.
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.

Field	Values	Additional Information
OSPF Neighbors		
Address	Address of the neighbor.	
Interface	Interface through which the neighbor is reachable.	
State	State of the neighbor: Attempt, Down, Exchange, ExStart, Full, Init, Loading, or 2way.	Generally, only the Down state, indicating a failed OSPF adjacency, and the Full state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.
ID	Router ID of the neighbor.	
Priority	Priority of the neighbor to become the designated router.	
Dead	Number of seconds until the neighbor becomes unreachable.	
OSPF Interfaces		
Interface	Name of the interface running OSPF.	
State	State of the interface: BDR, Down, DR, DRother, Loop, PtToPt, or Waiting.	The Down state, indicating that the interface is not functioning, and PtToPt state, indicating that a point-to-point connection has been established, are the most common states.
Area	Number of the area that the interface is in.	
DR ID	Address of the area's designated router.	
BDR ID	Address of the area's backup designated router.	
Nbrs	Number of neighbors on this interface.	
OSPF Statistics		
Packet Type	Type of OSPF packet.	
Total Sent/Total Received	Total number of packets sent and received.	
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.	
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.	

Field	Values	Additional Information
Routes learned	Number of RIP routes learned on the logical interface.	
Routes advertised	Number of RIP routes advertised on the logical interface.	
RIP Neighbors		
Neighbor	Name of the RIP neighbor.	This value is the name of the interface on which RIP is enabled. The name is set in 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 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 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 51 summarizes key output fields in service sets displays.

Table 51: 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

Firewall information is divided into multiple parts:

- To view stateful firewall information in the J-Web interface, select **Monitor > Firewall > Stateful Firewall**. To display firewall 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

- To view intrusion detection service (IDS) information, 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 52, and click **OK**.

Table 52: 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 53 summarizes key output fields in firewall and IDS displays.

Table 53: Summary of Key Firewall and IDS Output Fields

Field	Values
Stateful Firewall	
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.
Direction	Direction of the flow: I (input) or O (output).
Frames	Number of frames in the flow.
IDS Information	
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 ike security-associations

Table 54 summarizes key output fields in IPSec displays.

Table 54: Summary of Key IPSec Output Fields

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

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 55 summarizes key output fields in NAT displays.

Table 55: 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.

Field	Values
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.

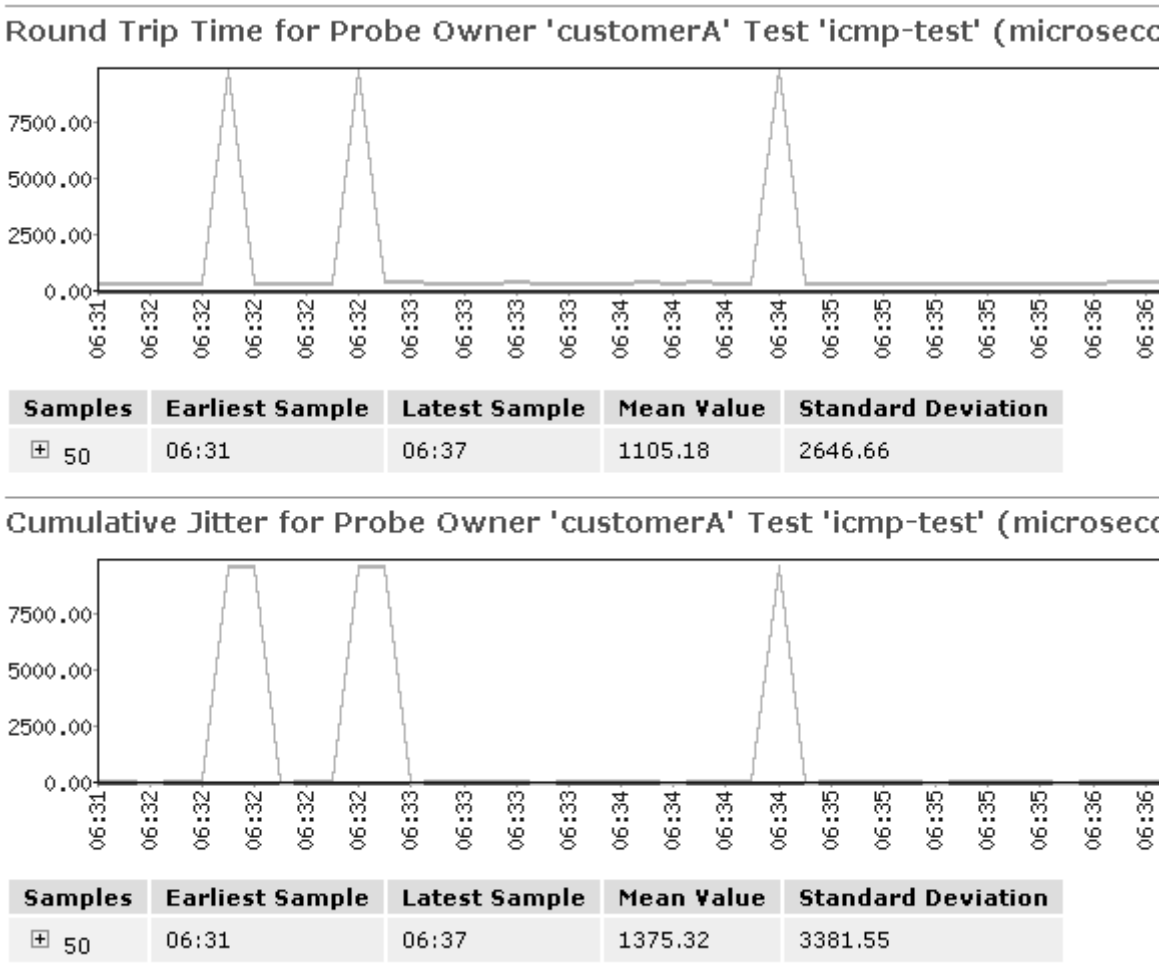
Monitoring RPM Probes

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 shows sample graphs for an RPM test.

Figure 11: Sample RPM Graphs



In Figure 11, 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 56 summarizes key output fields in RPM displays.

Table 56: Summary of Key RPM Output Fields

Field	Values	Additional Information
Currently Running Tests		
Graph		Click the **Graph** link to display the graph (if it is not already displayed) or to update the graph for a particular test.
Owner	Configured owner name of the RPM test.	

Field	Values	Additional Information
Test Name	Configured name of the RPM test.	
Probe Type	Type of RPM probe configured for the specified test. Following are valid probe types: ■ http-get ■ http-get-metadata ■ icmp-ping ■ icmp-ping-timestamp ■ tcp-ping ■ udp-ping	
Target Address	IP address or URL of the remote server that is being probed by the RPM test.	
Source Address	Explicitly configured source address that is included in the probe packet headers.	If no source address is configured, the RPM probe packets use the outgoing interface as the source address, and the Source Address field is empty.
Minimum RTT	Shortest round-trip time from the Services Router to the remote server, as measured over the course of the test.	
Maximum RTT	Longest round-trip time from the Services Router to the remote server, as measured over the course of the test.	
Average RTT	Average round-trip time from the Services Router to the remote server, as measured over the course of the test.	
Standard Deviation RTT	Standard deviation of round-trip times from the Services Router to the remote server, as measured over the course of the test.	
Probes Sent	Total number of probes sent over the course of the test.	
Loss Percentage	Percentage of probes sent for which a response was not received.	
Round-Trip Time for a Probe		
Samples	Total number of probes used for the data set.	The Services Router maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	
Latest Sample	System time when the last probe in the sample was received.	
Mean Value	Average round-trip time for the 50–probe sample.	
Standard Deviation	Standard deviation of the round-trip times for the 50–probe sample.	

Field	Values	Additional Information
Lowest Value	Shortest round-trip time from the Services Router to the remote server, as measured over the 50–probe sample.	
Time of Lowest Sample	System time when the lowest value in the 50–probe sample was received.	
Highest Value	Longest round-trip time from the Services Router to the remote server, as measured over the 50–probe sample.	
Time of Highest Sample	System time when the highest value in the 50–probe sample was received.	
Cumulative Jitter for a Probe		
Samples	Total number of probes used for the data set.	The Services Router maintains records of the most recent 50 probes for each configured test. These 50 probes are used to generate RPM statistics for a particular test.
Earliest Sample	System time when the first probe in the sample was received.	
Latest Sample	System time when the last probe in the sample was received.	
Mean Value	Average jitter for the 50–probe sample.	
Standard Deviation	Standard deviation of the jitter values for the 50–probe sample.	
Lowest Value	Smallest jitter value, as measured over the 50–probe sample.	
Time of Lowest Sample	System time when the lowest value in the 50–probe sample was received.	
Highest Value	Highest jitter value, as measured over the 50–probe sample.	
Time of Highest Sample	System time when the highest jitter value in the 50–probe sample was received.	

Using J-Web Diagnostic Tools

This section contains the following topics:

Using the J-Web Ping Host Tool

You can use the ping host diagnostic tool to verify that a 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 "Using the ping Command" on page 126.)

To use the ping host tool:

1. Select **Diagnose** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 12).
3. Enter information into the Ping Host page, as described in Table 57.

   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 13). 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 58 summarizes the output fields of the display.
5. To stop the ping operation before it is complete, click **OK**.

Figure 12: Ping Host Page

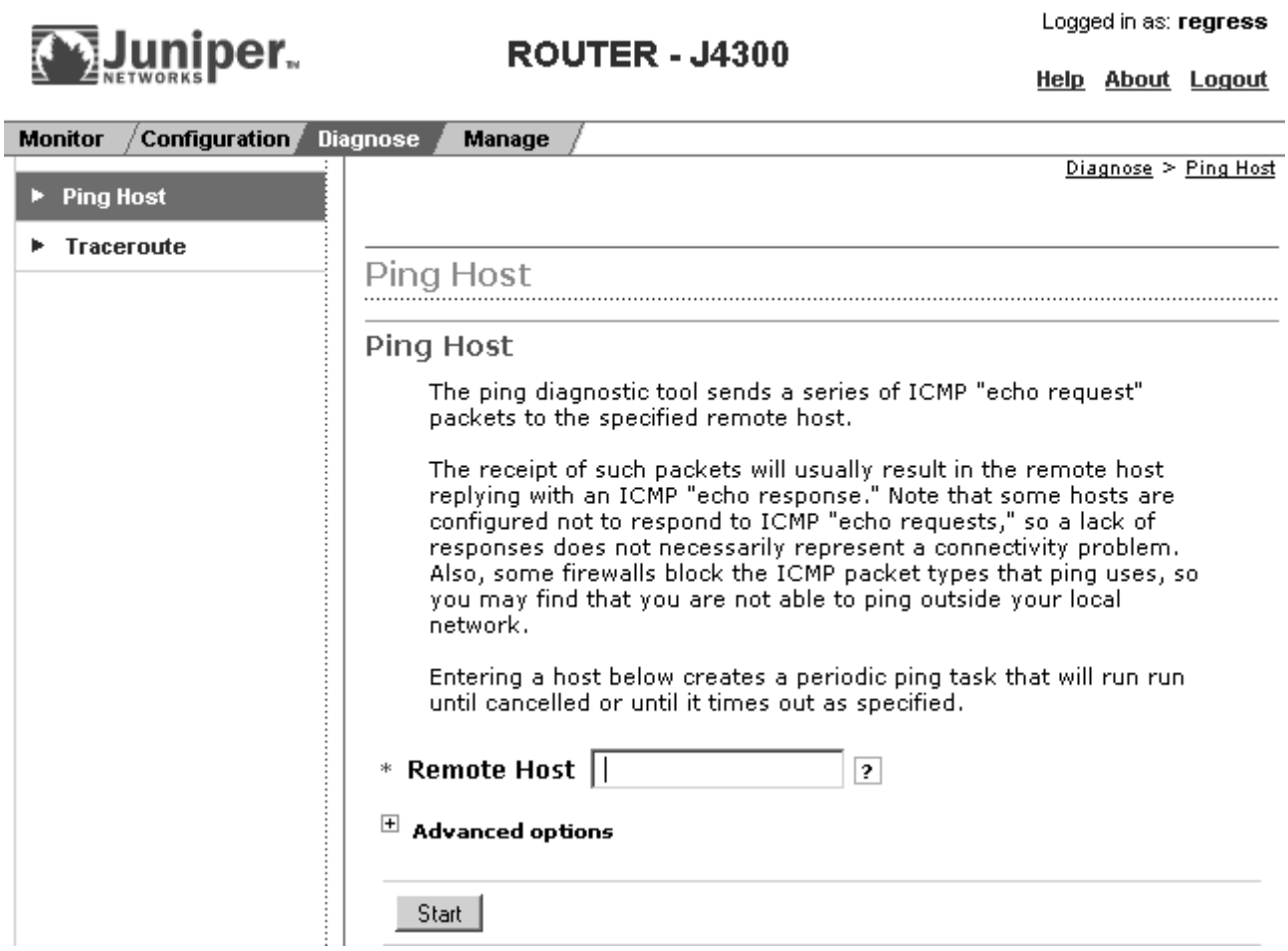


Table 57: J-Web Ping Host Summary

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.
Interval	Specifies the interval, in seconds, between the transmission of each ping request.	From the drop-down 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.

Field	Function	Your Action
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 drop-down 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.
Interface	Specifies the interface on which the ping requests are sent.	From the drop-down 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 drop-down 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.
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 drop-down list, select the decimal value of the TOS field.

Figure 13: Ping Host Results Page

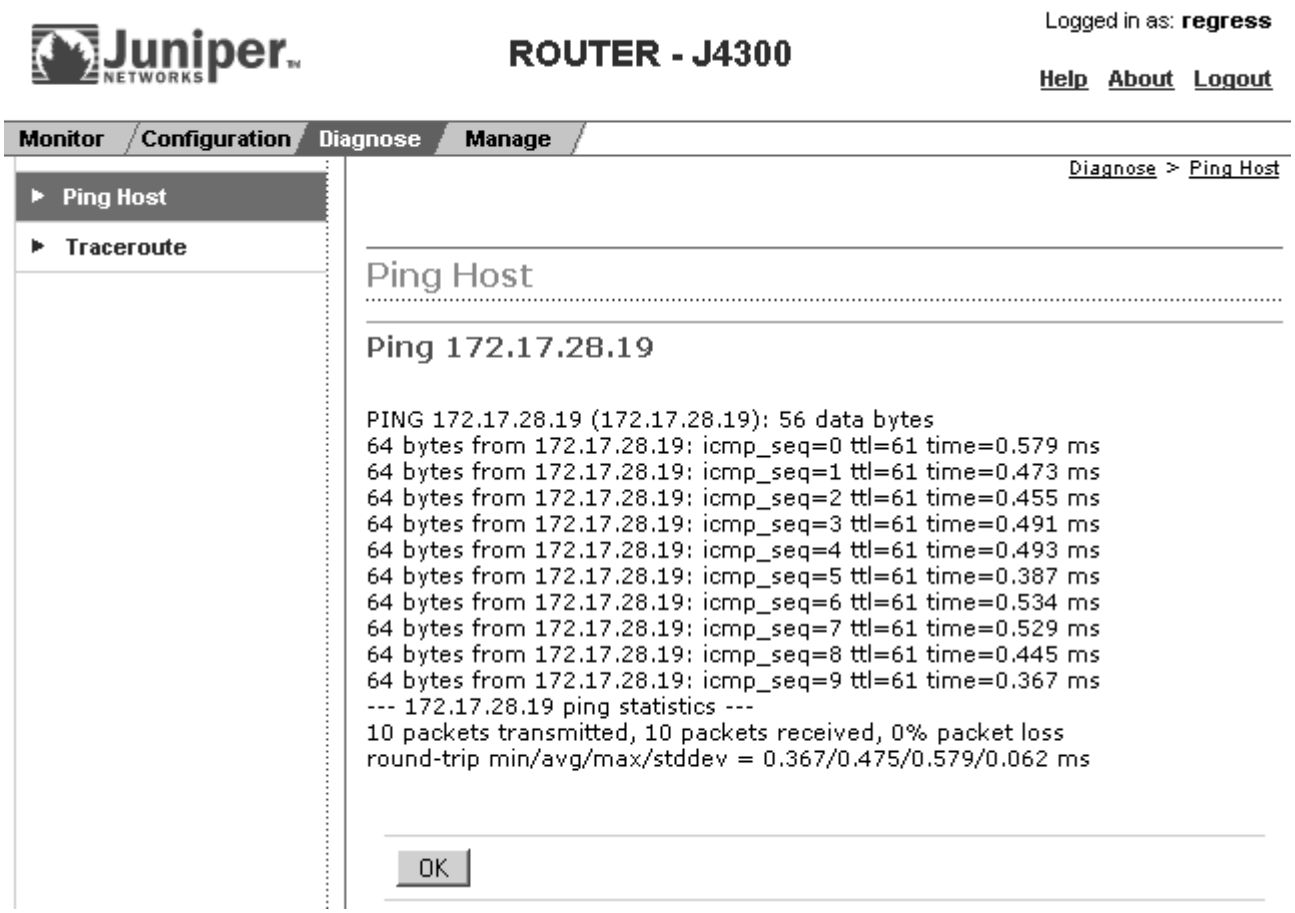


Table 58: J-Web Ping Host Results Summary

Field	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=*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.
number packets transmitted	*number* —Number of ping requests (probes) sent to host.
number packets received	*number* —Number of ping responses received from host.

Field	Description
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 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

You can use the ping MPLS diagnostic tool to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 VPNs, and Layer 2 circuits.

When you issue a command 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.

Alternatively, you can use the CLI commands ping mpls, ping mpls l2circuit, ping mpls l2vpn, and ping mpls l3vpn. For more information, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

Options for Checking MPLS Connections

The ping MPLS diagnostic tool has eight options for returning information about MPLS connections in VPNs and LSPs. Table 59 lists and explains the options for checking MPLS connections.

Table 59: Options for Checking MPLS Connections

Ping MPLS Tool	Purpose	Additional Information
Ping RSVP-signaled LSP	Checks the operability of an LSP that has been set up by RSVP. The Services Router pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the Services Router sends the ping requests on the path that is currently active.
Ping LDP-signaled LSP	Checks the operability of an LSP that has been set up using 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	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	Checks the operability of the connections related to a Layer 2 VPN. The Services Router directs outgoing request probes out the specified interface.	
Instance to which this connection belongs	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	Checks the operability of the Layer 2 circuit connections. The Services Router directs outgoing request probes out the specified interface.	

Ping MPLS Tool	Purpose	Additional Information
Locate LSP from virtual circuit information	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	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.	

Ping MPLS Requirements

Before using the ping MPLS tool, make sure that your network meets the following requirements:

- 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 Configuration Guide*.

- 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 Configuration Guide* to configure the loopback address.

- 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."

Using the Ping MPLS Tool

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 14).
3. Enter information into the Ping MPLS page, as described in Table 60.
4. Click **Start**.

Table 61 summarizes the output fields of the display.

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

Figure 14: Ping MPLS Page

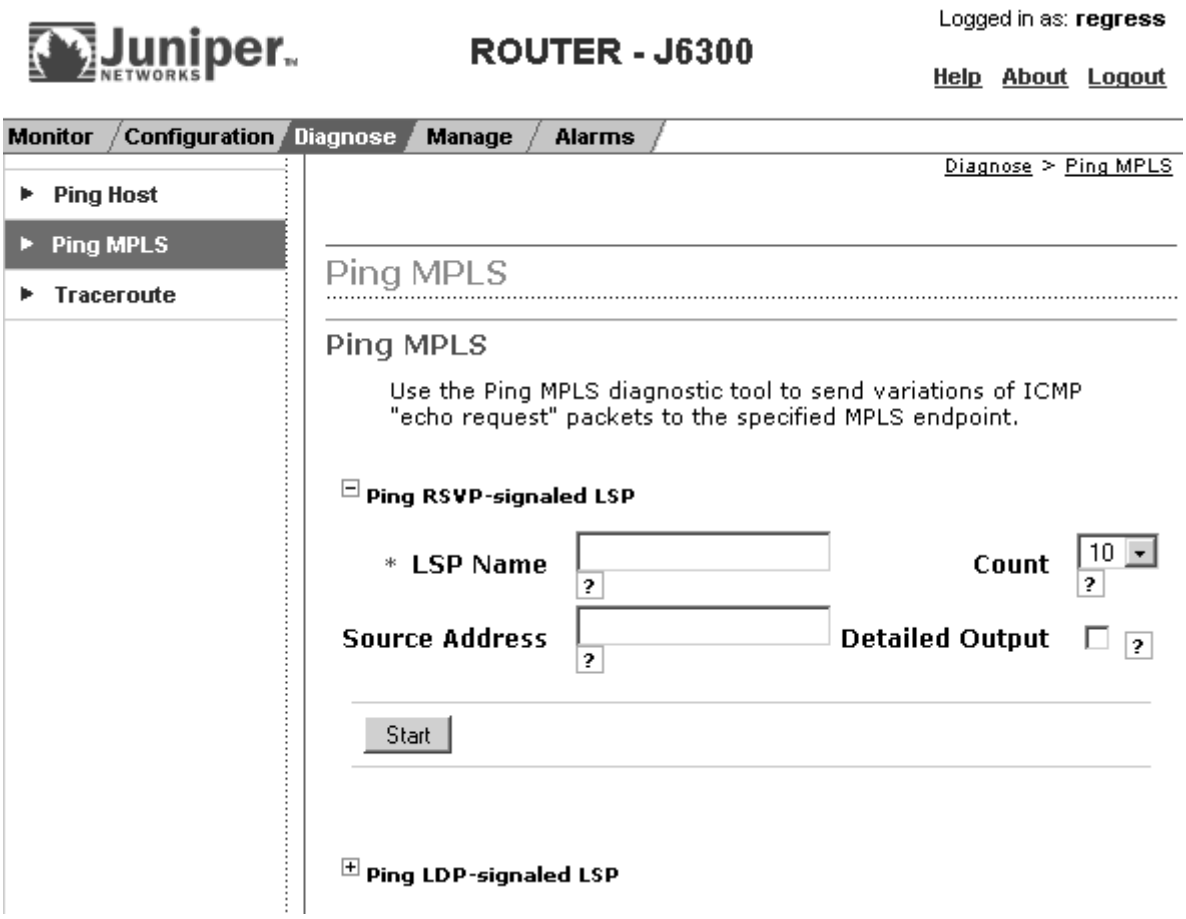


Table 60: J-Web Ping MPLS Summary

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 drop-down list, select the number of ping requests to send. The default is 5 requests.

Field	Function	Your Action
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
Ping LDP-signaled LSP		
FEC Prefix	Identifies the LSP to ping.	Type the forwarding equivalence class (FEC) prefix and length of the LSP to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a Services Router interface.
Count	Specifies the number of ping requests to send.	From the drop-down 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 drop-down list, select the number of ping requests to send. The default is 5 requests.
Detailed Output	Requests the display of extensive rather than brief ping output.	Select the check box to display detailed output.
VPN Prefix	Identifies the IP address prefix and length of the Layer 3 VPN to ping.	Type the IP address prefix and length of the VPN to ping.
Source Address	Specifies the source address of the ping request packet.	Type the source IP address—a valid address configured on a Services Router interface.
Locate LSP using interface name		
Interface	Specifies the interface on which the ping requests are sent.	From the drop-down 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 drop-down 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 drop-down list, select the number of ping requests to send. The default is 5 requests.

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 drop-down 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 drop-down 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 drop-down 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 drop-down 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.

Table 61: J-Web Ping MPLS Results 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.

Field	Description
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.

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 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.

Using the J-Web Traceroute Tool

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. (See "Using the traceroute Command" on page 128.)

To use the traceroute tool:

1. Select **Diagnose > Traceroute**.
2. Next to Advanced options, click the expand icon (see Figure 15).
3. Enter information into the Traceroute page, as described in Table 62.

   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 63 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 15: Traceroute Page

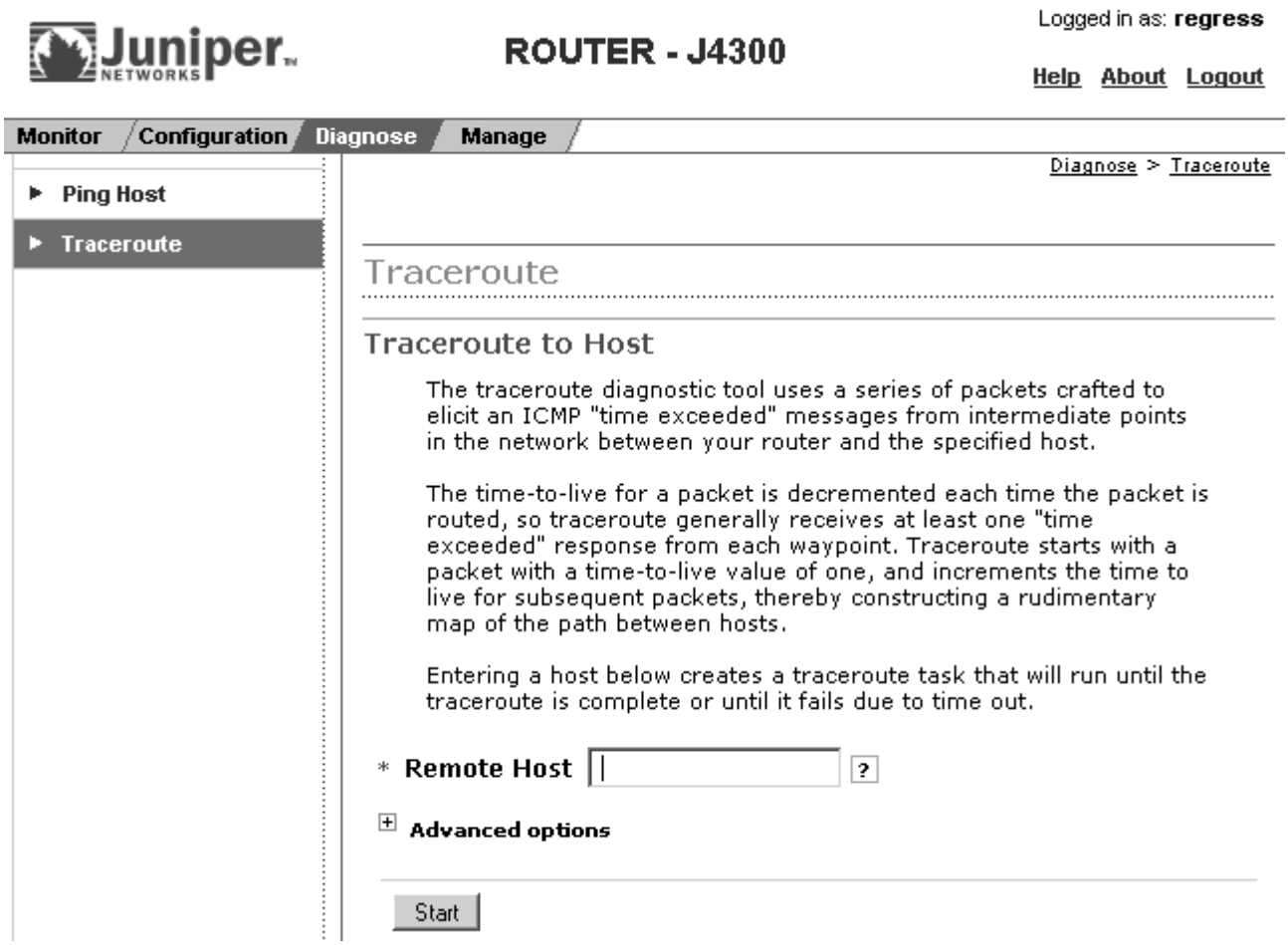


Table 62: Traceroute Summary

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.

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 drop-down 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 drop-down 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 drop-down 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.

Table 63: J-Web Traceroute Results 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 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*.

Using CLI Diagnostic Commands

This section describes how to use the CLI diagnostic tools. 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 89.

This section contains the following topics:

Using the ping Command

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 112.)

Enter the ping command with the following syntax. Table 64 describes the ping command options.

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

To quit the ping command, press Ctrl-C.

Table 64: CLI ping Command Options

Option	Description
host	Pings the hostname or IP address you specify.
interface *source-interface*	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	Bypasses the routing tables and send 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.
count *number*	Limits the number of ping requests to send. Specify a count from 0 through 1,000,000. If you do not specify a count, ping requests are continuously sent until you press Ctrl-C.
do-not-fragment	Sets the Don't Fragment (DF) bit in the IP header of the ping request packet.
inet	Forces the ping requests to an IPv4 destination.
interval *seconds*	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*]	Sets the loose source routing option in the IP header of the ping request packet.
no-resolve	Suppresses the display of the hostnames of the hops along the path.
pattern *string*	Includes the hexadecimal string you specify, in the ping request packet.
rapid	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	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*	Uses the routing instance you specify for the ping request.
size *bytes*	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 *address*	Uses the source address that you specify, in the ping request packet.
strict	Sets the strict source routing option in the IP header of the ping request packet.
strict-source [*hosts*]	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*	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*	Sets the time-to-live (TTL) value for the ping request packet. Specify a value from 0 through 255.

Option	Description
verbose	Displays detailed output.
wait *seconds*	Sets the maximum time to wait after sending the last ping request packet.
detail	Displays the interface on which the ping response was received.

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. Table 58 summarizes these output fields.

Using the traceroute Command

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 "Using the J-Web Traceroute Tool" on page 122.)

Enter the traceroute command with the following syntax. Table 65 describes the traceroute command options.

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

To quit the traceroute command, press Ctrl-C.

Table 65: CLI traceroute Command Options

Option	Description
host	Sends traceroute packets to the hostname or IP address you specify.
interface *source-interface*	Sends the traceroute packets on the interface you specify. If you do not include this option, traceroute packets are sent on all interfaces.
as-number-lookup	Displays the autonomous system (AS) number of each intermediate hop between the router and the destination host.
bypass-routing	Bypasses the routing tables and send 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.
gateway *address*	Uses the gateway you specify to route through.
logical-router *logical-router-name*	Sends traceroute packets to this logical router.
inet	Forces the traceroute packets to an IPv4 destination.
no-resolve	Suppresses the display of the hostnames of the hops along the path.
routing-instance *routing-instance-name*	Uses the routing instance you specify for the traceroute.
source *address*	Uses the source address you specify in the traceroute packet.
tos *number*	Sets the type-of-service (TOS) value in the IP header of the traceroute packet. Specify a value from 0 through 255.
ttl *number*	Sets the time-to-live (TTL) value for the traceroute packet. Specify a hop count from 0 through 255.
wait *seconds*	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. Table 63 summarizes these output fields.

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 66 and Table 67 list the keys you use to control the display using the *interface-name* and traffic options. (The keys are not case sensitive.)

Table 66: 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 67: CLI monitor interface Traffic Output Control Keys

Key	Action
b	Displays the statistics in units of bytes and bytes per second (bps).
c	Clears (returns to 0) the delta counters in the Delta column. The statistics counters are not cleared.
d	Displays the Delta column instead of the rate column—in bps or packets per second (pps).
p	Displays the statistics in units of packets and packets per second (pps).
q or ESC	Quits the command and returns to the command prompt.
r	Displays the rate column—in bps and pps—instead of the Delta column.

Following are sample displays from the monitor interface command:

```
    user@host> monitor interface fe-0/0/0
host1                           Seconds: 11                 Time: 16:47:49
                                                            Delay: 0/0/0
Interface: fe-0/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 100mbps
Traffic statistics:                                      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.

Enter the monitor traffic command with the following syntax. Table 68 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.

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.

Table 68: CLI monitor traffic Command Options

Option	Description
absolute-sequence	Displays the absolute TCP sequence numbers.
count *number*	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*	Displays packet headers for traffic on the specified interface. If an interface is not specified, the lowest numbered interface is monitored.
layer2-headers	Displays the link-layer packet header on each line.

Option	Description
matching *expression*	Displays packet headers that match an expression. Table 69 through Table 71 list match conditions, logical operators, and arithmetic, binary, and relational operators you can use in the expression.
no-domain-names	Suppresses the display of the domain name portion of the hostname.
no-promiscuous	Specifies *not* to place the monitored interface in promiscuous mode. In promiscuous mode, the interface reads every packet that reaches it. In non-promiscuous mode, the interface reads only the packets addressed to it.
no-resolve	Suppresses the display of hostnames.
no-timestamp	Suppresses the display of packet header timestamps.
print-ascii	Displays each packet header in ASCII format.
print-hex	Displays each packet header, except link-layer headers, in hexadecimal format.
size *bytes*	Displays the number of bytes for each packet that you specify. If a packet header exceeds this size, the displayed packet header is truncated. The default value is 96.
brief	Displays minimum packet header information. This is the default.
detail	Displays packet header information in moderate detail. For some protocols, you must also use the size option to see detailed information.
extensive	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 69, enclosed in quotation marks (“ “). You can combine match conditions by using the logical operators listed in Table 70 (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 71 (listed from highest to lowest precedence):

- Arithmetic—Expressions that use the arithmetic operators listed in Table 71.
- Binary—Expressions that use the binary operators listed in Table 71.
- Packet data accessor—Expressions that use the following syntax:

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

Replace *protocol* with any protocol in Table 69. 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 69: CLI monitor traffic Match Conditions

Match Condition	Description
Entity Type	
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.

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

Table 70: CLI monitor traffic Logical Operators

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

Table 71: CLI monitor traffic Arithmetic, Binary, and Relational Operators

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

Operator	Description
=	A match occurs if the first expression is equal to the second.
!=	A match occurs if the first expression is not equal to the second.

Following is sample output from the monitor traffic command:

```
    user@host> monitor traffic count 4 matching “arp” detail
Listening on fe-0/0/0, capture size 96 bytes

15:04:16.276780  In arp who-has 193.1.1.1 tell host1.site2.net
15:04:16.376848  In arp who-has host2.site2.net tell host1.site2.net
15:04:16.376887  In arp who-has 193.1.1.2 tell host1.site2.net
15:04:16.601923  In arp who-has 193.1.1.3 tell host1.site2.net
```

Using the monitor file Command

You can enter the monitor file command to display real-time additions to files such as 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.

Using mtrace Commands

You can use CLI mtrace commands to trace information about multicast paths. This section covers the following mtrace commands:

- mtrace from-source—Displays information about a multicast path from a source to a receiver. See “Using the mtrace from-source Command” on page 135.
- mtrace monitor—Monitors and displays multicast trace operations. See “Using the mtrace monitor Command” on page 137.

For more information about the mtrace commands, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

Using the mtrace from-source Command

To display information about a multicast path from a source to a receiver, enter the mtrace from-source command with the following syntax. Table 72 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> | <ttl number> |
<wait-time seconds>> <loop> <multicast-response | unicast-response>
<no-resolve> <no-router-alert> <brief | detail>
```

Table 72: CLI mtrace from-source Command Options

Option	Description
source *host*	Traces the path to the specified hostname or IP address.
extra-hops *number*	Sets the number of extra hops to trace past nonresponsive routers. Specify a value from 0 through 255.
group *address*	Traces the path for the specified group address. The default value is 0.0.0.0.
interval *seconds*	Sets the interval between statistics gathering. The default value is 10.
max-hops *number*	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*	Sets the maximum number of queries for any hop. Specify a value from 1 through 32. The default value is 3.
response *host*	Sends the response packets to the specified hostname or IP address. By default, the response packets are sent to the router that sent the requests.
ttl *number*	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*	Sets the time to wait for a response packet. The default value is 3 seconds.
loop	Loops indefinitely, displaying rate and loss statistics. To quit the mtrace command, press Ctrl-C.
multicast-response	Forces the responses to use multicast.
unicast-response	Forces the response packets to use unicast.
no-resolve	Does not display hostnames.
no-router-alert	Does not use the router alert IP option in the IP header.
brief	Does not display packet rates and losses.
detail	Displays packet rates and losses if a group address is specified.

Following is sample output from the mtrace from-source command:

```
    user@host> mtrace from-source source 192.1.4.1 group 224.1.1.1
Mtrace from 192.1.4.1 to 192.1.30.2 via group 224.1.1.1
Querying full reverse path... * *
  0  ? (192.1.30.2)
 -1  ? (192.1.30.1)  PIM  thresh^ 1
 -2  routerC.mycompany.net (192.1.40.2)  PIM  thresh^ 1
 -3  hostA.mycompany.net (192.1.4.1)
Round trip time 22 ms; total ttl of 2 required.

Waiting to accumulate statistics...Results after 10 seconds:

  Source        Response Dest    Overall     Packet Statistics For Traffic From
192.1.4.1  192.1.30.2       Packet      192.1.4.1 To 224.1.1.1
```

```
     v       __/  rtt   16 ms     Rate       Lost/Sent = Pct  Rate
192.168.195.37
192.1.40.2      routerC.mycompany.net
     v     ^      ttl    2                      0/0    = --    0 pps
192.1.40.1
192.1.30.1      ?
     v      \__   ttl    3                      ?/0            0 pps
192.1.30.2      192.1.30.2
  Receiver      Query Source
```

Each line of the trace display is usually in the following format (depending on the options selected and the responses from the routers along the path):

```
hop-number  host ( ip-address ) protocol ttl
```

Table 73 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 73: CLI mtrace from-source Command Display 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 74 summarizes the output fields of the display.

Table 74: CLI mtrace monitor Command Display 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.

Chapter 7

Monitoring Real-Time Performance

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 75.

Table 75: RPM Terms

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

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
- ICMP timestamp request to a target address
- UDP ping packets to a target
- TCP ping packets to a target

UDP and TCP probe types require that the remote server be configured as an RPM receiver so that it generates responses to the probes.

RPM Tests

Each probed target is monitored over the course of a test. A test represents a collection of probes, sent out at regular intervals, as defined in the configuration. Statistics are then returned for each test. Because a test is a collection of probes that have been monitored over some amount of time, test statistics such as standard deviation and jitter can be calculated and included with the average probe statistics.

Probe and Test Intervals

Within a test, RPM probes are sent at regular intervals, configured in seconds. When the total number of probes have been sent and the corresponding responses received, the test is complete. You can manually set the probe interval for each test to control how the RPM test is conducted.

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

RPM Statistics

At the end of each test, the Services Router collects the statistics for packet round-trip time, packet inbound and outbound times (for ICMP timestamp probes only), and probe loss shown in Table 76.

Table 76: 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

RPM Statistics	Description
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
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.

Before You Begin

Before you begin configuring RPM, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See the *J-series Services Router 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 RPM parameters. Figure 16 shows the main Quick Configuration page for RPM. Figure 17 shows the probe test Quick Configuration page for RPM.

Figure 16: Main Quick Configuration Page for RPM

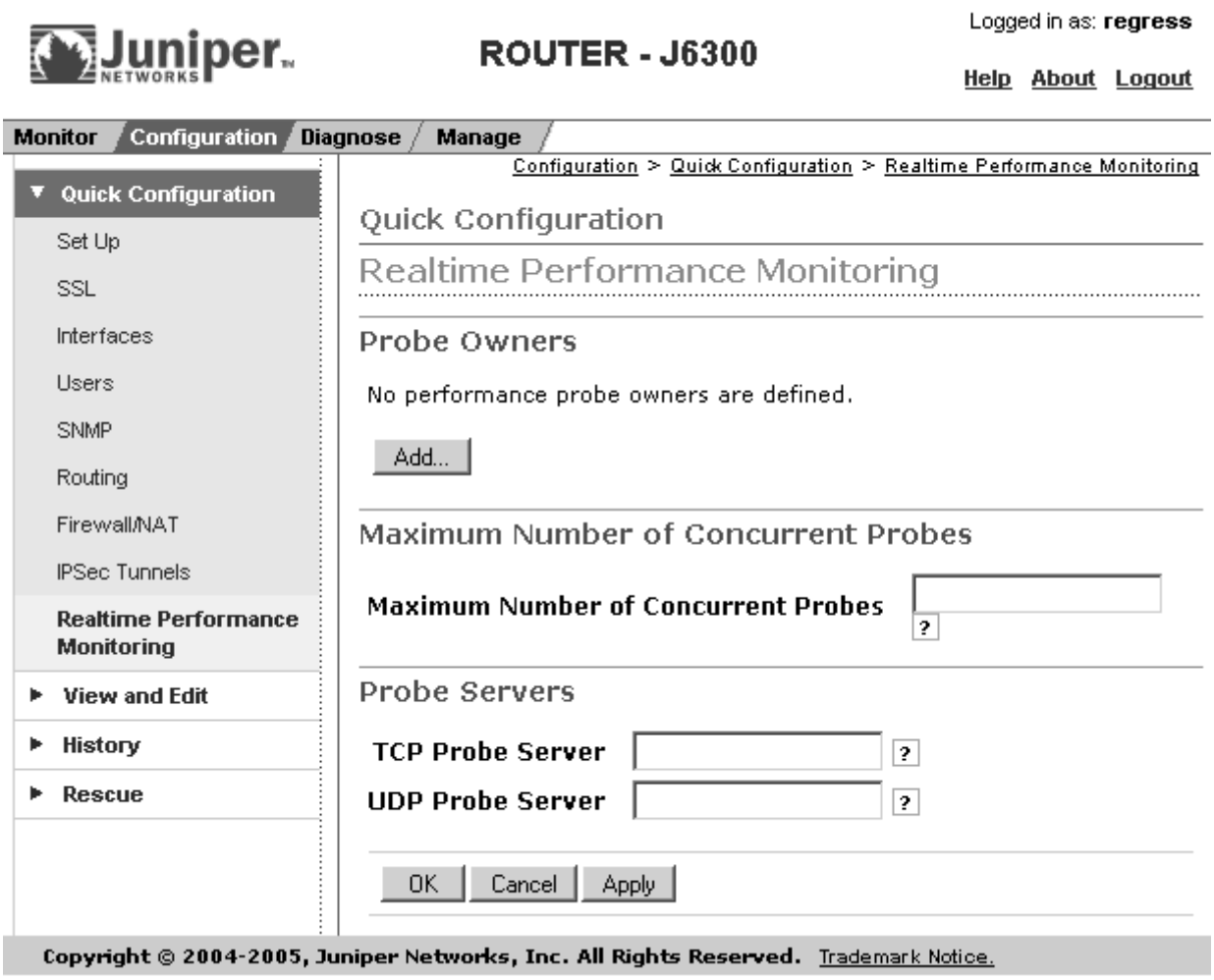
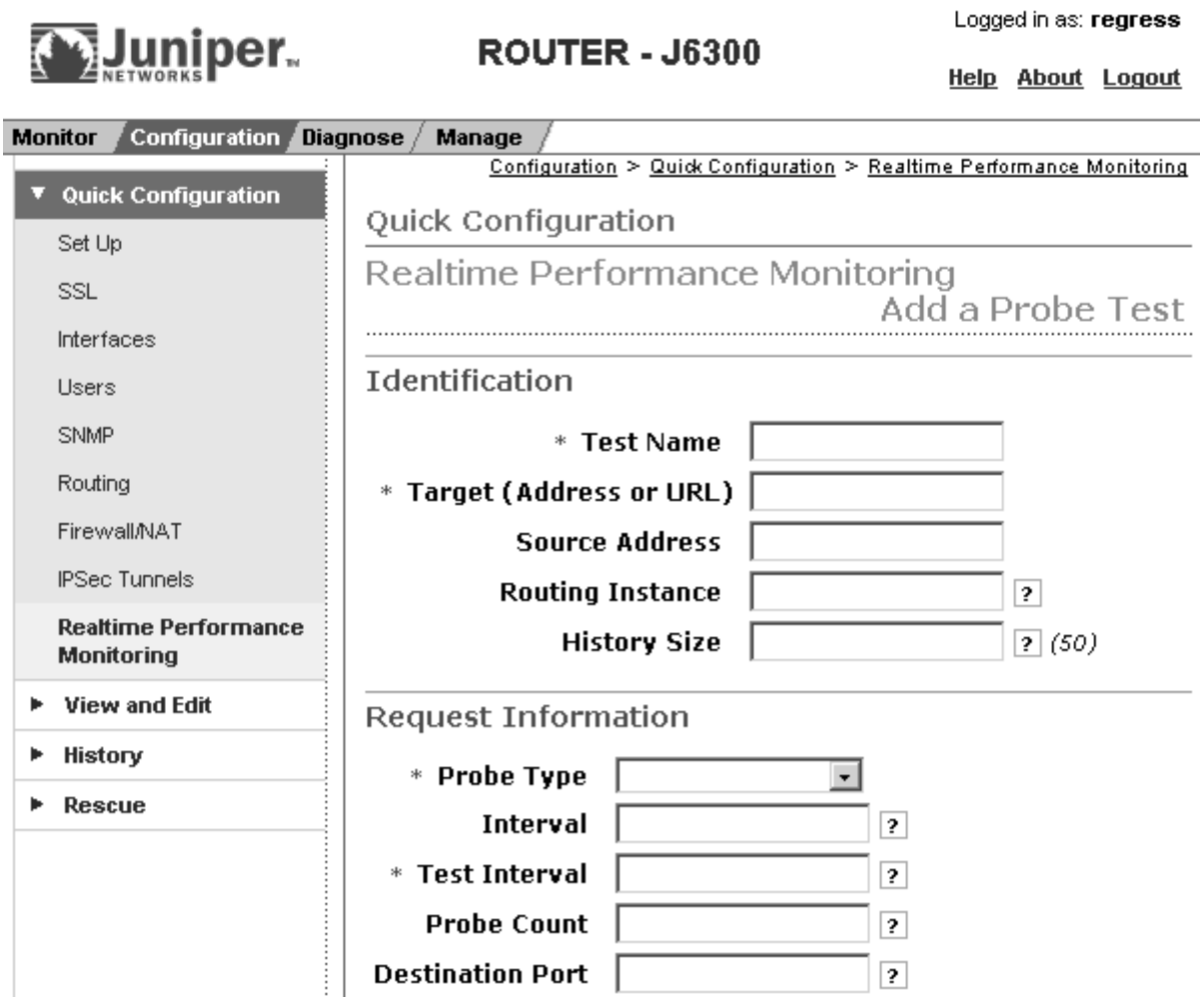


Figure 17: Probe Test Quick Configuration Page for RPM



To configure RPM parameters with Quick Configuration:

1. In the J-Web user interface, select **Configuration > RPM**.
2. Enter information into the Quick Configuration page for RPM, as described in Table 77.
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 156.

Table 77: 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 drop-down menu: ■ **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).

Field	Function	Your Action
Probe Count	Sets the total number of probes to be sent for each test.	Type a number between 1 and 15.
Destination Port	Specifies the TCP or UDP port to which probes are sent. To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server (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 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 to use as the contents of the ICMP probe data.
Maximum Probe Thresholds		
Successive Lost Probes	Sets the total number of probes that must be lost successively to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Lost Probes	Sets the total number of probes that must be lost to trigger a probe failure and generate a system log message.	Type a number between 0 and 15.
Round Trip Time	Sets the total round-trip time (in microseconds), from the Services Router to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Jitter	Sets the total jitter (in microseconds), for a test, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds) for a test, which, if exceeded, triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).
Egress Time	Sets the total one-way time (in microseconds), from the Services Router to the remote server, that triggers a probe failure and generates a system log message.	Type a number between 0 and 60,000,000 (microseconds).

Field	Function	Your Action
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.
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.

Field	Function	Your Action
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 must perform the following tasks marked *(Required)*. For information about using the J-Web and CLI configuration editors, see the *J-series Services Router Configuration Guide*.

Configuring Basic RPM Probes (Required)

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

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

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 78.
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 (Optional)" on page 153.
   - To tune a probe, see "Tuning RPM Probes (Optional)" on page 154.
   - To check the configuration, see "Verifying an RPM Configuration" on page 156.

Table 78: 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 configuration editor hierarchy, select **Services**. 2. Select the **Yes** check box. 3. Click **Configure**.	From the top of the configuration hierarchy, enter edit services rpm

Task	J-Web Configuration Editor	CLI Configuration Editor
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 above 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, and a target address of 192.178.16.5.	1. In the configuration editor hierarchy, select **customerA**. 2. In the Test box, click **Add new entry** 3. In the Name box, type icmp-test. 4. In the Probe frequency box, type 15. 5. In the Probe type box, select **icmp-ping-timestamp**. 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 192.178.16.5. 9. Click **OK**.	1. From the top of the configuration hierarchy, 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 target address 192.178.16.5
Configure RPM thresholds and corresponding SNMP traps to catch ingress (inbound) times greater than 3000 microseconds.	1. In the configuration editor hierarchy, 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

Task	J-Web Configuration Editor	CLI Configuration Editor
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. In the configuration editor hierarchy, select **customerB**. 2. In the Test box, click **Add new entry**. 3. In the Name box, type http-test. 4. In the Probe frequency 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 top of the configuration hierarchy, 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
Configure RPM thresholds and corresponding SNMP traps to catch 3 or more successive lost probes and total lost probes of 10 or more.	1. In the configuration editor hierarchy, 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 (Optional)

To configure RPM using TCP and UDP probes, in addition to the basic RPM properties, you must configure both the host Services Router and the remote Services Router to act as TCP and UDP servers.

In this sample use of RPM, a probe is configured for one customer: Customer C. The probe for Customer C uses TCP packets. The remote router is configured as an RPM server for both TCP and UDP packets, using ports 50000 and 50037, respectively. Router A is the host router in this example, and router B is the remote router. To configure this RPM probe:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 79.
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 (Optional)" on page 154.
   - To check the configuration, see "Verifying an RPM Configuration" on page 156.

Table 79: 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 configuration editor hierarchy, select **Services**. 2. Select the **Yes** check box. 3. Click **Configure**.	From the top of the configuration hierarchy, 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

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the RPM test tcp-test for the RPM owner customerC. The sample RPM test is a TCP probe with a test interval (probe frequency) of 5, a probe type of tcp-ping, and a target address of 192.162.45.6.	1. In the configuration editor hierarchy, select **customerC**. 2. In the Test box, click **Add new entry**. 3. In the Name box, type tcp-test. 4. In the Probe frequency 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 top of the configuration hierarchy, enter edit services rpm probe customerC 2. Enter set test tcp-test probe-frequency 5 3. Enter set test tcp-test probe-type tcp-ping 4. Enter set test tcp-test target address 192.162.45.6
Configure port 50000 as the TCP port to which the RPM probes are sent.	In the Destination port box, type 50000.	Enter set test tcp-test destination-port 50000
Router B Configuration		
Navigate to the **Services > RPM** level in the configuration hierarchy.	1. In the configuration editor hierarchy, select **Services**. 2. Select the Yes check box. 3. Click **Configure**.	From the top of the configuration hierarchy, enter edit services rpm
Configure Router B to act as a TCP server, using port 50000 to send and receive TCP probes.	1. In the configuration editor hierarchy, select **Probe Server**. 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. In the configuration editor hierarchy, select **Probe Server**. 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 (Optional)

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 (Required)" on page 150.

To configure tune RPM probes:

1. Perform the configuration tasks described in Table 78.
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 80.
4. If you are finished configuring the network, commit the configuration.
5. To check the configuration, see "Verifying an RPM Configuration" on page 156.

Table 80: Tuning RPM Probes

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **Services > RPM** level in the configuration hierarchy.	1. In the configuration editor hierarchy, select **Services**. 2. Select the **Yes** check box. 3. Click **Edit**.	From the top of the configuration hierarchy, enter edit services rpm
Set the maximum number of concurrent probes allowed on the system to 10.	In the Probe limit box, type 10.	Enter set probe-limit 10
Navigate to the **Services > RPM > Probe > CustomerA > Test > Icmp-test** level in the configuration hierarchy.	1. In the configuration editor hierarchy, select **Services**. 2. Select the **Yes** check box. 3. Click **Edit**. 4. In the Probe box, click icmp-test.	From the top of the configuration hierarchy, enter edit services rpm probe customerA test icmp-test
Set the time between probe transmissions to 30 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.	In the Source address box, type 192.168.2.9.	Enter set source-address 192.168.2.9

Verifying an RPM Configuration

To verify an RPM configuration, perform these tasks:

- Verifying RPM Statistics on page 156
- Verifying RPM Probe Servers on page 157

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.

Sample Output

```
user@host> show services rpm probe-results

   Owner: customerA, Test: icmp-test
    Probe type: icmp-ping-timestamp
    Minimum Rtt: 312 usec, Maximum Rtt: 385 usec, Average Rtt: 331 usec,
    Jitter Rtt: 73 usec, Stddev Rtt: 27 usec
    Minimum egress time: 0 usec, Maximum egress time: 0 usec,
    Average egress time: 0 usec, Jitter egress time: 0 usec,
    Stddev egress time: 0 usec
    Minimum ingress time: 0 usec, Maximum ingress time: 0 usec,
    Average ingress time: 0 usec, Jitter ingress time: 0 usec,
    Stddev ingress time: 0 usec
    Probes sent: 5, Probes received: 5, Loss percentage: 0

    Owner: customerB, Test: http-test
    Target address: 192.176.17.4, Target URL: http://customerB.net,
    Probe type: http-get
    Minimum Rtt: 1093 usec, Maximum Rtt: 1372 usec, Average Rtt: 1231 usec,
    Jitter Rtt: 279 usec, Stddev Rtt: 114 usec
    Probes sent: 3, Probes received: 3, Loss percentage: 0
```

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).

For more information about show services rpm probe-results, see the *JUNOS Network and Services Interfaces 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.

Sample Output

```
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.

For more information about show services rpm active-servers, see the *JUNOS Network and Services Interfaces Command Reference*.

Chapter 8

Performing Software Upgrades and Reboots

To upgrade the JUNOS Internet software on a Services Router, you install a new version that you download from the Web to a remote server or your computer. Use either the J-Web interface or the CLI to perform the upgrade.

If you need to replace the primary boot device or add a backup boot device on the router, you can configure a boot device with the CLI or with a UNIX or Microsoft Windows computer. You can also configure a boot device to receive core dumps.

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

For more information about installing and upgrading JUNOS software, see the *JUNOS System Basics Configuration Guide*.

Upgrade Overview

The Services Router is delivered with the JUNOS Internet software preinstalled. To upgrade the software, you use the J-Web interface or CLI commands to copy a set of software images over the network to memory storage on the Routing Engine.

All junos-jseries software is delivered in signed packages that contain Secure Hash Algorithm 1 (SHA-1) checksums. A package is installed only if the SHA-1 checksum within it matches the SHA-1 hash recorded in its corresponding .sha1 file. (For example, -export.tgz contains -export.tgz and

-export.tgz.sha1. The junos-jseries-*release*-export.tgz package is installed only if the SHA-1 hashes match in the two -export.tgz.sha1 files.)

The junos-jseries package completely reinstalls the software. This package rebuilds the file system but retains configuration files, log files, and similar information from the previous version.

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 upgrading, be sure to back up the currently running and active file system and configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. To back up the file system, you must have a removable compact flash drive installed on the J4300 or J6300 Services Router, or a USB storage device installed on any J-series Services Router.

To back up the file system to the removable compact flash drive, issue the following command:

user@host> **request system snapshot media removable-compact-flash**

To back up the file system to the removable USB storage device, issue the following command:

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

For details about the request system snapshot command, see "Configuring Boot Devices with the CLI" on page 169.

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. Choose either **Canada and U.S. Version** or **Worldwide Version**:
   - https://www.juniper.net/support/csc/swdist-domestic/
   - https://www.juniper.net/support/csc/swdist-ww/
2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Using either the J-Web interface or the CLI, choose the software package for your application.

4. Download the software to a local host.

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

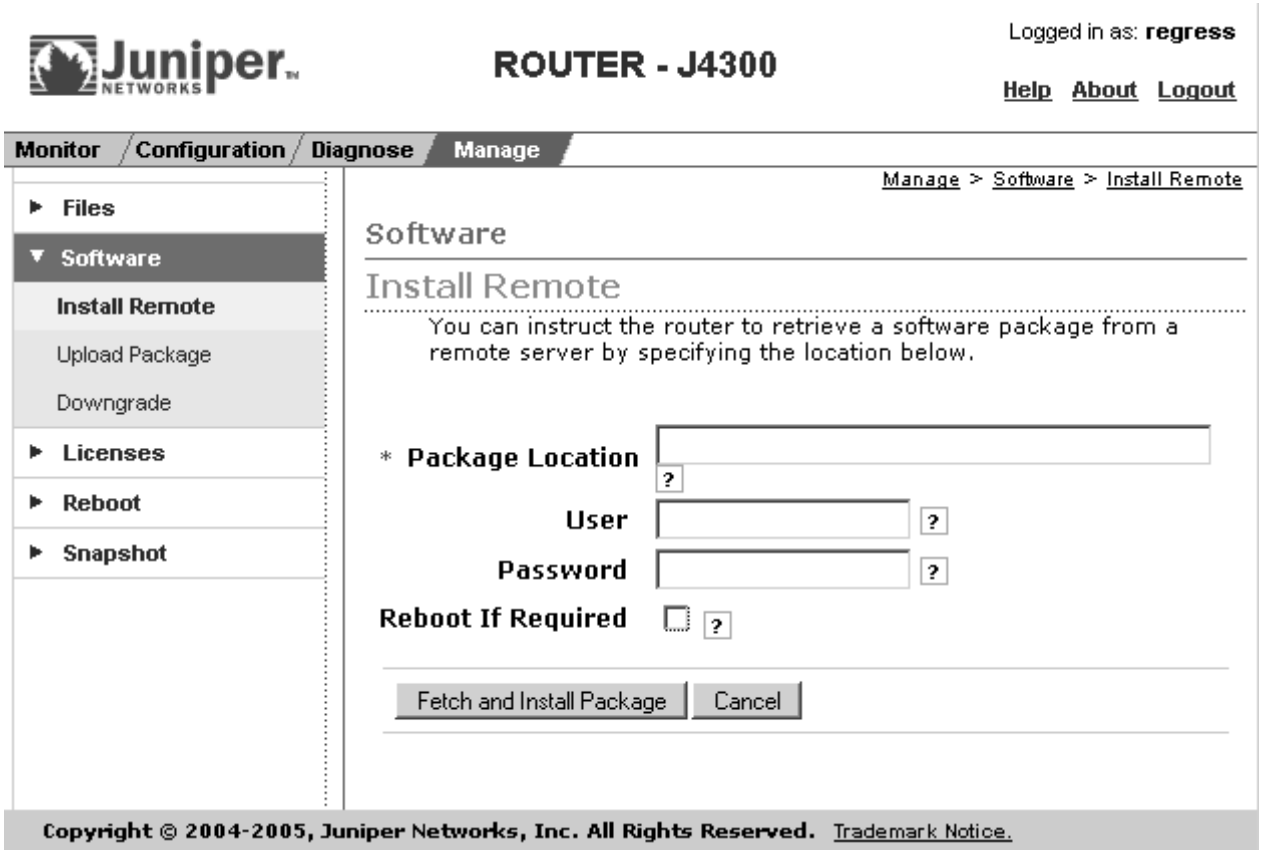
You can use the J-Web interface to install software upgrades from a remote server using FTP or HTTP, or by uploading the file to the router. This section contains the following topics:

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 18 shows the Install Remote page for the router.

Figure 18: 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 160.
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. Download the software to your local host or internal software distribution site.
4. In the J-Web interface, select **Manage > Software > Install Remote**.
5. On the Install Remote page, enter information into the fields described in Table 81.
6. Click **OK**. The software is activated after the router has rebooted.

Table 81: Install Remote Summary

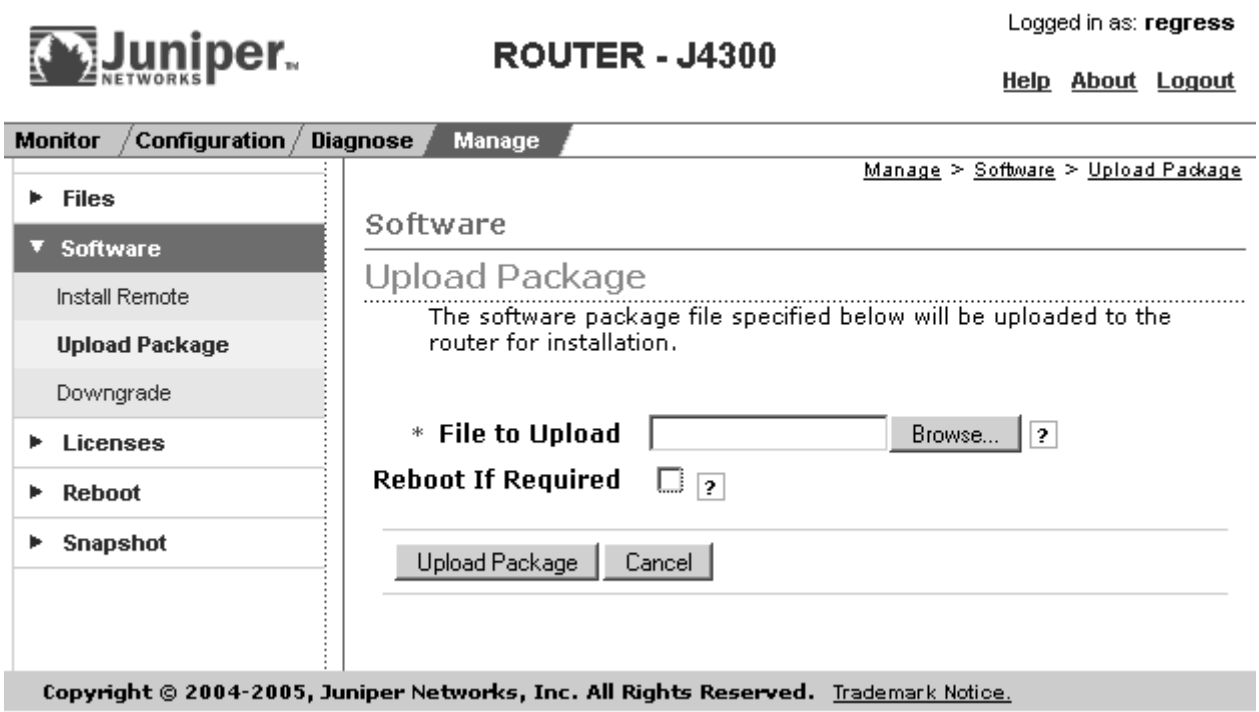
Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server on which the software package resides.	Type the full address of the software package location on the FTP or HTTP server.
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to reboot automatically when the upgrade is complete.

Installing Software Upgrades by Uploading Files

You can use the J-Web interface to install software packages uploaded from your computer to the Services Router.

Figure 19 shows the Upload Package page for the router.

Figure 19: 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 160.
2. In the J-Web interface, select **Manage > Software > Upload Package**.
3. Enter information into the fields described in Table 82 into the Upload Package page.
4. Click **Upload Package**. The software is activated after the router has rebooted.

Table 82: 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 using the CLI:

1. Download the software package as described in "Downloading Software Upgrades from Juniper Networks" on page 160.
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:
   - Customers in the United States and Canada use the following command:

     user@host> **request system software add validate** *path* **/junos-jseries** *release* **-domestic.tgz**

   - All other customers use the following command:

     user@host> **request system software add validate** *path* **/junos-jseries** *release* **-export.tgz**

   Replace *path* with the full pathname to the bundle. Replace *release* with the software release version of the bundle.
4. Reboot the router to activate the junos-jseries software:

   user@host> **request system reboot**

```
Reboot the system ? [yes,no] (no) yes
Shutdown NOW!
```

All the software is activated when you issue the reboot command.

The router then reboots from the primary boot device on which you just installed the software. When the reboot is complete, the router displays the login prompt.

5. If your compact flash is running out of space and you do not wish to downgrade the software to a previous version, you can recover up to 30 MB of space by using the request system software delete-backup CLI command. This command deletes the backup software package.

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

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 can not 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. 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 *J-series Services Router Getting Started Guide*.

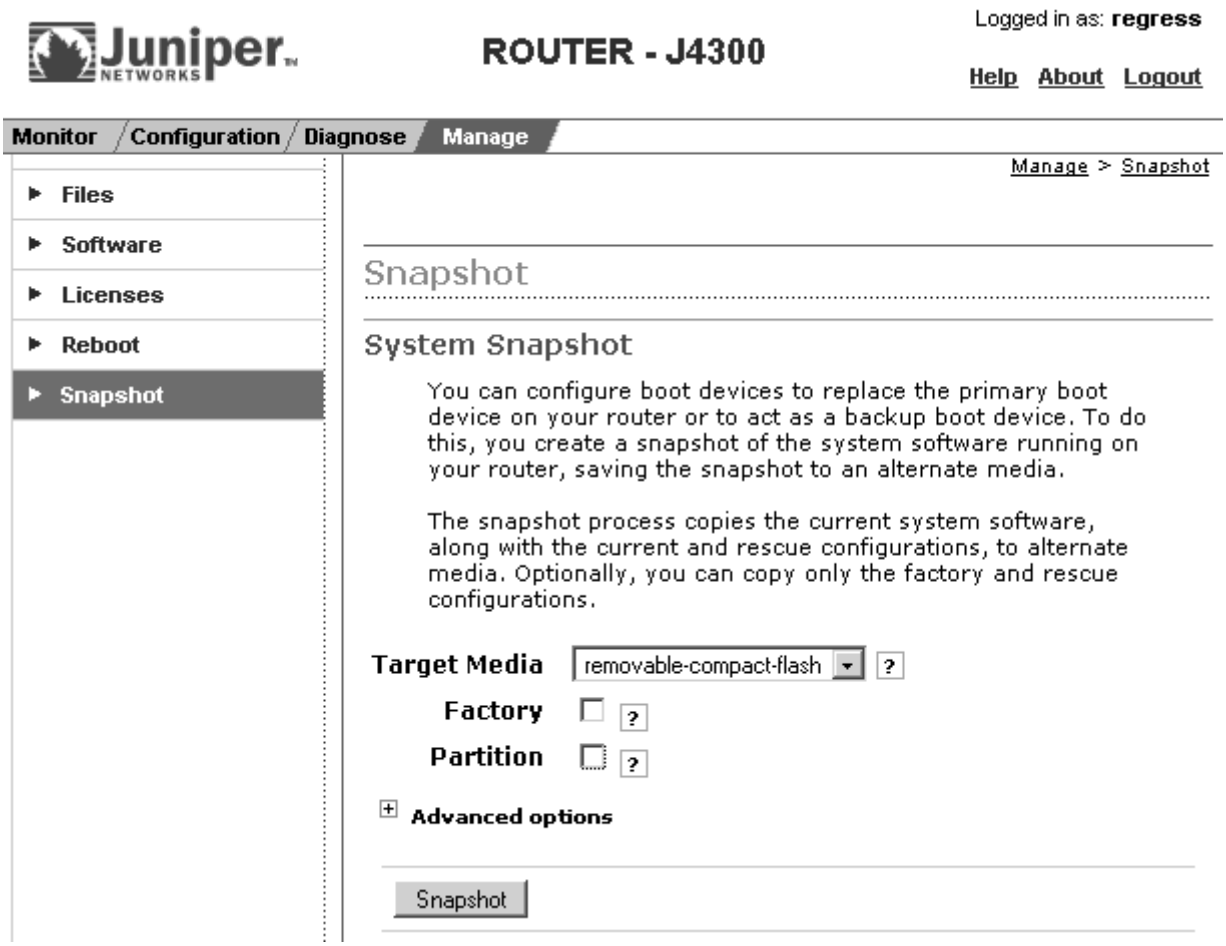
This section contains the following topics:

Configuring Boot Devices 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 20 shows the Snapshot page.

Figure 20: 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 83.
3. Click **Snapshot**.
4. Click **OK**.

Table 83: 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 drop-down list, select a boot device that is not the active boot device: ■ **compact-flash**—Copies software to the primary compact flash drive. ■ **removable-compact-flash**—Copies software to the removable compact flash drive. This option is available on J4300 and J6300 Services Routers only. ■ **usb**—Copies software to the device connected to the USB port.
Factory	Copies only default files that were loaded on the primary compact flash drive when it was shipped from the factory, plus the rescue configuration, if one has been set. **NOTE:** After a boot device is created with the default factory configuration, it can operate only in a primary compact flash drive 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 a removable 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 primary compact flash drive 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 a primary compact flash drive, it can operate only in a primary compact flash drive slot.	To create a boot medium to use in the primary compact flash drive 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.

Field	Function	Your Action
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 174. 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.
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 Boot Devices 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 84 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 84: CLI request system snapshot Command Options

Option	Description
as-primary	On a removable 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 primary compact flash drive 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 a primary compact flash drive, it can operate only in a primary compact flash drive 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.
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 primary compact flash drive 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 primary compact flash drive slot.
media *type*	Specifies the boot device the software snapshot is copied to: ■ compact-flash—Copies software to the primary compact flash drive. ■ removable-compact-flash—Copies software to the removable compact flash drive. This option is available on J4300 and J6300 Services Routers only. ■ usb—Copies software to the device connected to the USB port. **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 174. **NOTE:** This option also partitions the boot medium.

Configuring Compact Flash Recovery

All Services Routers use a compact flash disk, or card, to store the JUNOS Internet software, router configuration files, and log files. The primary compact flash drive is not hot-swappable and is accessible only after you remove the cover on the back panel of the router chassis. In addition to the primary compact flash disk, J4300 and J6300 Services Routers have a slot in the front of the chassis for removable flash media. All Services Routers also support externally pluggable USB storage devices.

This section contains the following topics:

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 166.)

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

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

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

Recommended Recovery Hardware and Software

Before configuring compact flash recovery, assemble the equipment and software listed in Table 85.

Table 85: 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
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

Recovering Primary Compact Flash

To recover a primary compact flash disk with a corrupt or missing operating system, you must copy a special JUNOS software image directly to an unformatted (raw) device. Recovery images are available from the same location as normal J-series software upgrades. (See “Downloading Software Upgrades from Juniper Networks” on page 160.)

The images use the naming convention junos-jseries-*release*-cf*nnn*.gz, where *release* is the software version and *nnn* is the target compact flash disk size in megabytes—128, 256, or 512.

To recover a primary compact flash disk:

1. Plug the compact flash drive into a PCMCIA adapter or USB card reader on the host PC, and verify that it is recognized by the operating system.
2. Copy the JUNOS software image to the host PC and uncompress it with the compression utility.

The uncompressed image must have the same size as the target compact flash capacity: 128 MB, 256 MB, or 512 MB.

3. Copy the JUNOS software image to the compact flash disk 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 image to the compact flash disk, you can use it as the primary compact flash disk in any J-series Services Router. For installation instructions, see the *J-series Services Router Getting Started Guide*.

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 86 describes the set system dump-device command options.

Table 86: CLI set system dump-device Command Options

Option	Description
boot-device	Uses whatever device was booted from as the system software failure memory snapshot device.
compact-flash	Uses the primary compact flash as the system software failure memory snapshot device.
removable-compact-flash	Uses the compact flash device on the front of the router (J4300 and J6300 only) as the system software failure memory snapshot device.
usb	Uses the device attached to the USB port as the system software failure memory snapshot device.

Rebooting or Halting a Services Router

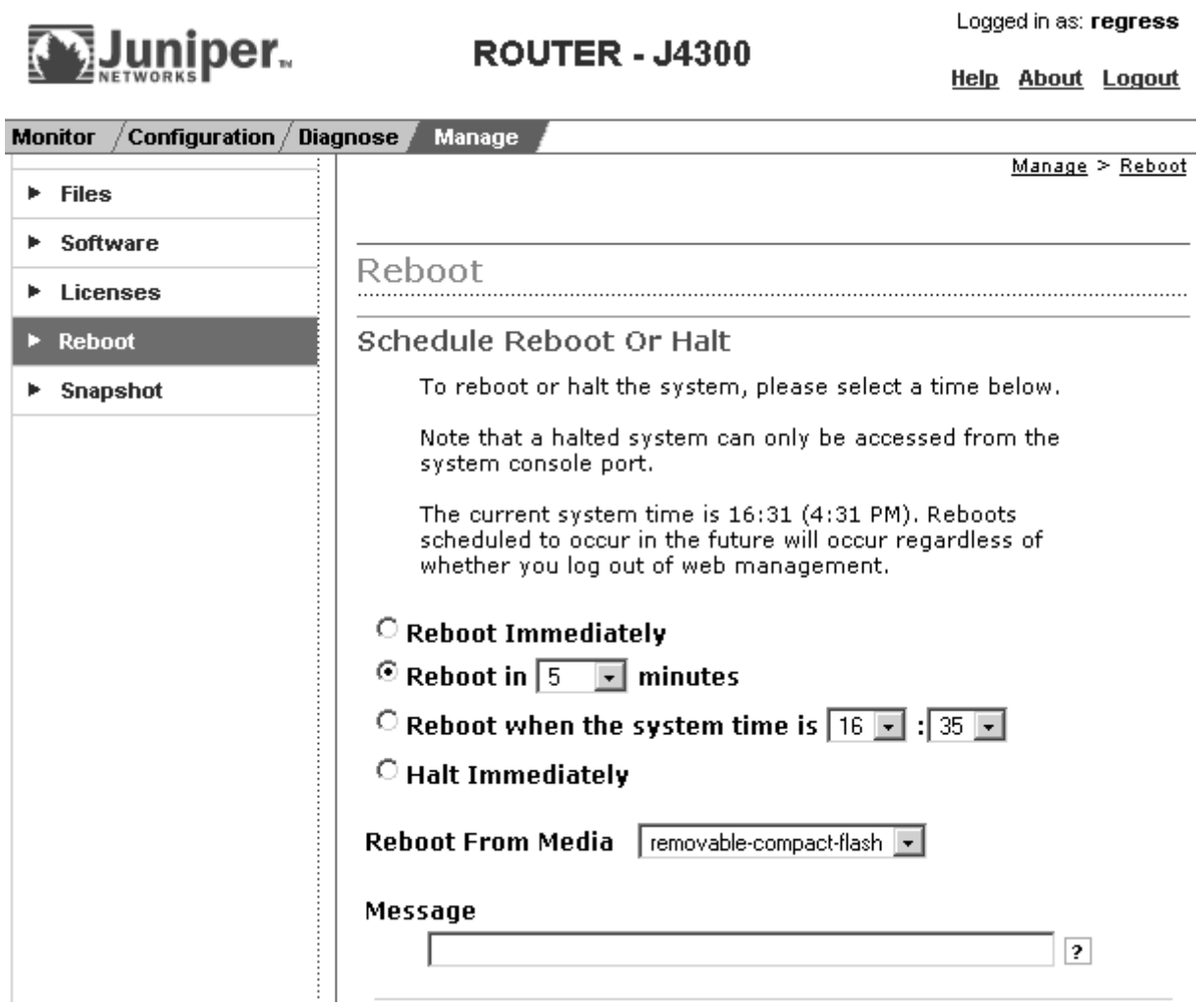
Reboot or halt a Services Router with either the J-Web interface or the CLI. This section contains the following topics:

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 21 shows the Reboot page for the router.

Figure 21: 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** drop-down menu:
   - **compact-flash**—Reboots from the primary compact flash drive. This selection is the default choice.
   - **removable-compact-flash**—Reboots from the optional removable compact flash drive. This selection is available on J4300 and J6300 Services Routers only.
   - **usb**—Reboots from the USB storage device.
4. (Optional) In the Message box, type a message to be displayed to any users on the router before the reboot occurs.
5. Click **Schedule**. The J-Web interface requests confirmation to perform the reboot or halt.
6. Click **OK** to confirm the operation.
   - If the reboot is scheduled to occur immediately, the router reboots. You cannot access the J-Web interface until the router has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.
   - If the reboot is scheduled to occur in the future, the Reboot page displays the time until reboot. You have the option to cancel the request by clicking **Cancel Reboot** on the J-Web interface Reboot page.
   - If the router is halted, all software processes stop and you can access the router through the console port only. Reboot the router by pressing any key on the keyboard.

NOTE: If you cannot connect to the router through the console port, shut down the router by pressing and holding the power button on the front panel until the POWER ON LED turns off. After the router has shut down, you can power on the router

by pressing the power button again. The POWER ON LED lights during startup and remains steadily green when the router is operating normally.

Rebooting the 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 87 describes the request system reboot command options.

Table 87: CLI Request System Reboot Command Options

Option	Description
none	Same as at now (reboots the router immediately).
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 primary compact flash drive. This is the default. ■ removable-compact-flash—Reboots from the optional removable compact flash drive. This option is available on J4300 and J6300 Services Routers only. ■ usb—Reboots from the USB storage device.
message *"text"*	Provides a message to display to all system users before the router reboots.

Halting the 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 ON LED turns off. After the router has shut down, you can power on the router by pressing the power button again. The POWER ON LED lights during startup and remains steadily green when the router is operating normally.

Table 88 describes the request system halt command options.

Table 88: CLI Request System Halt Command Options

Option	Description
none	Same as at now (stops software processes on the router immediately).
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 primary compact flash drive. This is the default. ■ removable-compact-flash—Reboots from the optional removable compact flash drive. This option is available on J4300 and J6300 Services Routers only. ■ usb—Reboots from the USB storage device.
message *"text"*	Provides a message to display to all system users before the software processes on the router are stopped.

Chapter 9

Contacting Customer Support and Returning Hardware

This chapter describes how to return the Services Router or individual components to Juniper Networks for repair or replacement. It contains the following topics:

Locating Component Serial Numbers

Before contacting Juniper Networks to request a Return Materials Authorization (RMA), you must find the serial number on the router or component. To list the router components and their serial numbers, enter the following command-line interface (CLI) command:

```
    user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN000192AB        J4300
Midplane         REV 02.04 710-010001  CORE99563
System IO        REV 02.03 710-010003  CORE100885        P12/P45 System IO board
Routing Engine   RevX2.6  750-010005   IWGS40735451      RE-J.2
FPC 0                                                   FPC
  PIC 0                                                 2x FE
```

NOTE: In the show chassis hardware output, PIMs are identified as PICs.

Most components also have a small rectangular serial number ID label (see Figure 22 through Figure 24) attached to the component body.

Figure 22: J2300 Serial Number ID Label

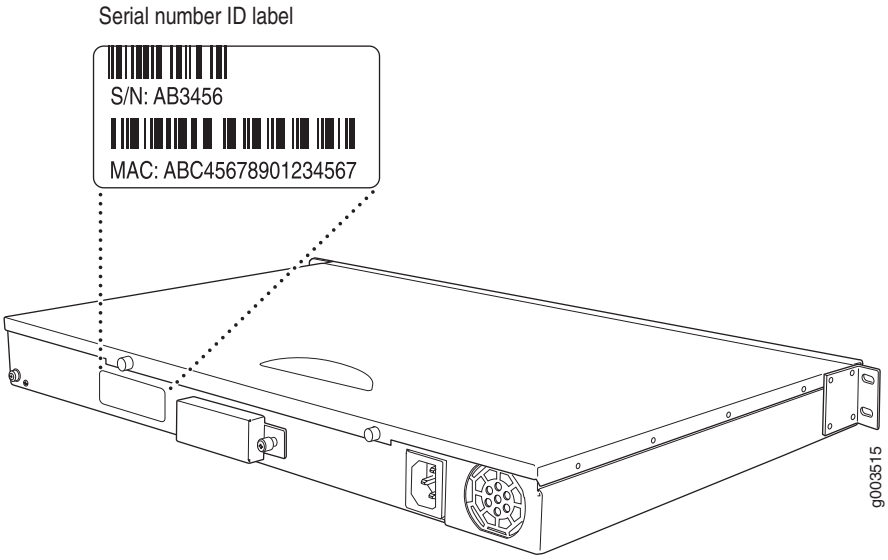


Figure 23: J4300 Serial Number ID Label

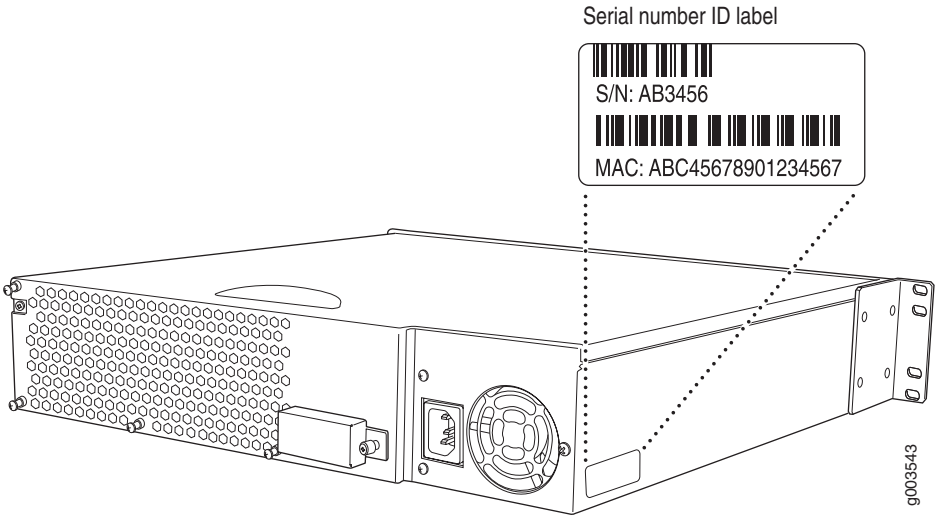
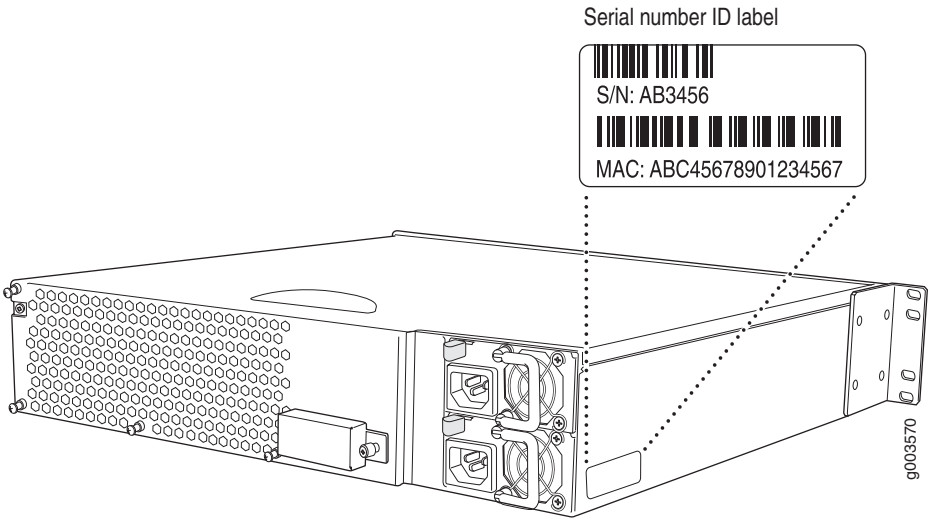


Figure 24: J6300 Serial Number ID Label



The following sections describe the label location on each type of component:

- PIM Serial Number Label on page 181
- J6300 Power Supply Serial Number Labels on page 181

PIM Serial Number Label

The PIMs installed in the J4300 and J6300 Services Routers are field-replaceable. Each PIM has a unique serial number. The serial number label is located on the right side of the PIM, when the PIM is horizontally oriented (as it would be installed in the router). The exact location may be slightly different on different PIMs, depending on the placement of components on the PIM board.

J6300 Power Supply Serial Number Labels

The power supplies installed in the J6300 Services Router are field-replaceable. Each power supply has a unique serial number. The serial number label is located on the top of the AC power supply.

Contacting Customer Support

After you have located the serial numbers of the components you need to return, contact Juniper Networks Technical Assistance Center (JTAC) in one of the following ways.

You can contact JTAC 24 hours a day, seven days a week.

- On the Web, using the Case Manager link at http://www.juniper.net/support/
- By telephone:

  From the US and Canada: 1-888-314-JTAC

  From all other locations: 1-408-745-9500

If contacting JTAC by telephone, enter your 11–digit case number followed by the pound (#) key if this is an existing case, or press the star (*) key to be routed to the next available support engineer.

Information You Might Need to Supply to JTAC

When requesting support from JTAC by telephone, be prepared to provide the following information:

- Your existing case number, if you have one
- Details of the failure or problem
- Type of activity being performed on the router when the problem occurred
- Configuration data displayed by one or more show commands

Return Procedure

If the problem cannot be resolved by the JTAC technician, an RMA number is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.

NOTE: Do not return any component to Juniper Networks unless you have first obtained an RMA number. Juniper Networks reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer via collect freight.

For more information about return and repair policies, see the customer support Web page at http:/www./juniper.net/support/guidelines.html.

For product problems or technical support issues, open a support case using the Case Manager link at http://www.juniper.net/support/, or call 1–888–314–JTAC (within the United States) or 1–408–745–9500 (outside the United States).

When you need to return a component, follow this procedure:

1. Determine the part number and serial number of the component. For instructions, see “Locating Component Serial Numbers” on page 179.

2. Obtain a Return Materials Authorization (RMA) number from the Juniper Networks Technical Assistance Center (JTAC). You can send e-mail or telephone as described above.

3. Provide the following information in your e-mail message or during the telephone call:

   - Part number and serial number of component
   - Your name, organization name, telephone number, and fax number
   - Description of the failure

4. The support representative validates your request and issues an RMA number for return of the component.

5. Pack the router or component for shipment, as described in "Packing a Router or Component for Shipment" on page 183.

Packing a Router or Component for Shipment

This section contains the following topics:

Tools and Parts Required

To remove components from the router or the router from a rack, you need the following tools and parts:

- Blank panels to cover empty slots
- Electrostatic bag or antistatic mat, for each component
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade screwdriver, approximately 1/4 in. (6 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Packing the Services Router for Shipment

To pack the router for shipment, follow this procedure:

1. Retrieve the shipping carton and packing materials in which the router was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.

2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see the *J-series Services Router Getting Started Guide*.

3. On the console or other management device connected to the master Routing Engine, enter CLI operational mode and issue the following command to shut down the router software.

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

   Wait until a message appears on the console confirming that the operating system has halted. For more information about the command, see "Halting the Services Router with the CLI" on page 177.

4. Shut down power to the router by pressing the power button on the front panel of the router.

5. Disconnect power from the router. For instructions, see the *J-series Services Router Getting Started Guide*.

6. Remove the cables that connect to all external devices. For instructions, see the *J-series Services Router Getting Started Guide*.

7. Remove all field-replaceable units (FRUs) from the router.

8. If the router is installed on a wall or rack, have one person support the weight of the router, while another person unscrews and removes the mounting screws.

9. Place the router in the shipping carton.

10. Cover the router with an ESD bag, and place the packing foam on top of and around the router.

11. Replace the accessory box on top of the packing foam.

12. Securely tape the box closed.

13. Write the RMA number on the exterior of the box to ensure proper tracking.

Packing Components for Shipment

To pack and ship individual components, follow these guidelines:

- When you return components, make sure they are adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place individual boards in electrostatic bags.
- Write the RMA number on the exterior of the box to ensure proper tracking.

CAUTION: Do not stack any of the router components.

Part 2

Index

Index

Symbols

A

B

C

D

E

F

G

H

I

J

M

N

O

P

Q

R

S

T

U

V

W

Y