



J-Web User Interface



Published: 2012-03-07

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

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

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

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

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

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

J-Web User Interface
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xiv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	J-Web User Interface	3
	J-Web Overview	3
	J-Web Layout	4
	Top Pane Elements	4
	Main Pane Elements	5
	Side Pane Elements	6
	Navigating the J-Web Interface	7
	Navigating the J-Web Configuration Editor	8
	Getting J-Web Help	8
Chapter 2	Installation and Setup	11
	J-Web Software Requirements	11
	Installing the J-Web Software	11
	Starting the J-Web Interface	12
	Configuring Basic Settings	14
Chapter 3	Secure Web Access	19
	Secure Web Access Overview	19
	Generating SSL Certificates	19
Part 2	Configuration	
Chapter 4	Configuration Tools	23
	Configuration Task Overview	23
	Point and Click CLI (J-Web Configuration Editor)	25
	CLI Viewer (View Configuration Text)	28
	CLI Editor (Edit Configuration Text)	29
	CLI Terminal Requirements	30
	Starting the CLI Terminal	31

	Using the CLI Terminal	32
Chapter 5	Configuration Tasks	35
	Editing and Committing a Junos OS Configuration	35
	J-Web Configuration Tasks	35
	Editing a Configuration	36
	Committing a Configuration	39
	Discarding Parts of a Candidate Configuration	39
	Accounting Options	40
Part 3	Administration	
Chapter 6	Session and User Management	45
	Setting J-Web Session Limits	45
	Terminating J-Web Sessions	46
	Viewing Current Users	46
Chapter 7	Secure Web Access	47
	Configuring Secure Web Access	47
Chapter 8	Alarms	51
	Using Alarms	51
	View Alarms	51
	Active Alarms Information	52
	Alarm Severity	52
	Displaying Alarm Descriptions	53
	Sample Task—Viewing and Filtering Alarms	53
Chapter 9	Events	55
	Using View Events	55
	Viewing Events	56
	View Events	56
	Understanding Severity Levels	57
	Using Filters	57
	Using Regular Expressions	59
	Sample Task—Filtering and Viewing Events	60
Chapter 10	Device Management	63
	Using Software (J Series Routing Platforms Only)	63
	Using Licenses (J Series Routing Platform Only)	64
	Using Snapshot (J Series Routing Platforms Only)	65
	Sample Task—Manage Snapshots	66
	Using Reboot	67
Chapter 11	Monitoring in J-Web	69
	Monitor Task Overview	69
	Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only)	70
	Class of Service	71
	Interfaces	72
	MPLS	73
	PPPoE (J Series Routing Platforms Only)	74
	RPM	74

	Routing	75
	Security	76
	Firewall	76
	IPsec	77
	NAT	77
	Service Sets	78
	Services	78
	System View	79
	System Information	79
	Chassis Information	79
	Process Details	80
	FEB Redundancy (M120 Routing Platforms Only)	80
	Sample Task—Monitoring Interfaces	81
	Sample Task—Monitoring Route Information	82
Chapter 12	Configuration and File Management	85
	Displaying Configuration History	85
	Displaying Users Editing the Configuration	87
	Loading a Previous Configuration File	88
	Downloading a Configuration File	89
	Comparing Configuration Files	89
	Upload Configuration File	90
	Using Rescue (J Series Routing Platforms Only)	91
	Using Files	92
Part 4	Troubleshooting	
Chapter 13	J-Web User Interface	95
	Lost Router Connectivity	95
	Unpredictable J-Web Behavior	95
	No J-Web Access	95
Chapter 14	Events	97
	Troubleshooting Events	97
Chapter 15	Network	99
	Using Ping Host	99
	Using Ping MPLS	100
	Using Ping ATM (M Series, MX Series, and T Series Routing Platforms Only) . . .	101
	Using Traceroute	102
	Using Packet Capture	102
	Sample Task—Ping Host	102
Part 5	Index	
	Index	109

List of Figures

Part 1	Overview	
Chapter 1	J-Web User Interface	3
	Figure 1: J-Web Layout	4
	Figure 2: Top Pane Elements	5
	Figure 3: Main Pane Elements	6
	Figure 4: Side Pane Elements	7
	Figure 5: CoS Help Page	9
Chapter 2	Installation and Setup	11
	Figure 6: J-Web Set Up Initial Configuration Page	15
Part 2	Configuration	
Chapter 4	Configuration Tools	23
	Figure 7: View Configuration Text Page	28
	Figure 8: Edit Configuration Text Page	29
	Figure 9: Starting the CLI Terminal	32
	Figure 10: J-Web CLI Terminal	34
Chapter 5	Configuration Tasks	35
	Figure 11: Edit Configuration Page	37
	Figure 12: Accounting Options Configuration Editor Page	41
Part 3	Administration	
Chapter 7	Secure Web Access	47
	Figure 13: Edit Management Access Page	47
Chapter 8	Alarms	51
	Figure 14: View Alarms Page	53
Chapter 9	Events	55
	Figure 15: View Events page	56
	Figure 16: J-Web View Events Page	61
Chapter 10	Device Management	63
	Figure 17: Manage Snapshots Page	67
Chapter 11	Monitoring in J-Web	69
	Figure 18: Chassis Viewer Page	71
	Figure 19: Sample RPM Graphs	75
	Figure 20: Port Monitoring Page	81
	Figure 21: Details of Interface ge-0/0/0 Page	82

	Figure 22: Monitoring Route Information Page with Complete Information	83
	Figure 23: Monitoring Route Information Page with Selective Information	83
Chapter 12	Configuration and File Management	85
	Figure 24: Configuration Database and History Page	86
	Figure 25: Database Information Page	88
	Figure 26: J-Web Configuration File Comparison Results	90
	Figure 27: J-Web Upload Configuration File Page	91
	Figure 28: Rescue Configuration Page	91
Part 4	Troubleshooting	
Chapter 14	Events	97
	Figure 29: View Events Page Displaying Error	97
	Figure 30: Verifying System Log Messages Configuration	98
Chapter 15	Network	99
	Figure 31: Ping Host Troubleshoot Page	103
	Figure 32: Successful Ping Host Results Page	104
	Figure 33: Unsuccessful Ping Host Results Page	105

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 1	Overview	
Chapter 1	J-Web User Interface	3
	Table 3: Key J-Web Edit Configuration Buttons	8
Chapter 2	Installation and Setup	11
	Table 4: Initial Configuration Set Up Summary	15
Part 2	Configuration	
Chapter 4	Configuration Tools	23
	Table 5: Junos OS Configuration Terms	24
	Table 6: J-Web Configuration Editor Tasks Summary	25
Chapter 5	Configuration Tasks	35
	Table 7: J-Web Configuration Tasks Summary	36
	Table 8: J-Web Edit Configuration Links	38
	Table 9: J-Web Edit Configuration Icons	38
	Table 10: J-Web Edit Configuration Buttons	39
Part 3	Administration	
Chapter 7	Secure Web Access	47
	Table 11: Secure Access Configuration Summary	48
Chapter 9	Events	55
	Table 12: Severity Levels	57
	Table 13: Summary of Event Filters	58
	Table 14: Common Regular Expression Operators and the Terms They Match	59
Chapter 10	Device Management	63
	Table 15: Manage Software Tasks Summary	64
Chapter 11	Monitoring in J-Web	69
	Table 16: Class of Service Information and the Corresponding CLI show Commands	72
	Table 17: Interfaces Information and the Corresponding CLI show Commands	73
	Table 18: MPLS Information and the Corresponding CLI show Commands	73

	Table 19: PPPoE Information and the Corresponding CLI show Commands	74
	Table 20: RPM Information and the Corresponding CLI show Command	74
	Table 21: Routing Information and the Corresponding CLI show Commands	75
	Table 22: Firewall Information and the Corresponding CLI show Commands	77
	Table 23: IPsec Information and the Corresponding CLI show Commands	77
	Table 24: NAT Information and the Corresponding CLI show Command	78
	Table 25: Service Sets Information and the Corresponding CLI show Commands	78
	Table 26: DHCP Information and the Corresponding CLI show Commands	78
	Table 27: System Information and the Corresponding CLI show Commands	79
	Table 28: Chassis Information and the Corresponding CLI show Commands	80
	Table 29: Process Details Information and the Corresponding CLI show Commands	80
	Table 30: FEB Redundancy Information and the Corresponding CLI show Command	80
Chapter 12	Configuration and File Management	85
	Table 31: J-Web Configuration History Summary	86
	Table 32: J-Web Configuration Database Information Summary	88
	Table 33: Manage Files Tasks Summary	92
Part 4	Troubleshooting	
Chapter 15	Network	99
	Table 34: Ping MPLS Tasks Summary and the Corresponding CLI show Commands	100
	Table 35: J-Web Ping Host Results and Output Summary	104

About the Documentation

- Documentation and Release Notes on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xiv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the [Junos OS CLI User Guide](#).

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons





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

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at

<https://www.juniper.net/cgi-bin/docbugreport/> . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

PART 1

Overview

- [J-Web User Interface on page 3](#)
- [Installation and Setup on page 11](#)
- [Secure Web Access on page 19](#)

CHAPTER 1

J-Web User Interface

- [J-Web Overview on page 3](#)
- [J-Web Layout on page 4](#)
- [Top Pane Elements on page 4](#)
- [Main Pane Elements on page 5](#)
- [Side Pane Elements on page 6](#)
- [Navigating the J-Web Interface on page 7](#)
- [Navigating the J-Web Configuration Editor on page 8](#)
- [Getting J-Web Help on page 8](#)

J-Web Overview

The J-Web interface allows you to monitor, configure, troubleshoot, and manage the routing platform by means of a Web browser enabled with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). J-Web provides access to all the configuration statements supported by the routing platform, so you can fully configure it without using the Junos OS CLI.

You can perform the following tasks with the J-Web interface:

- **Monitoring**—Display the current configuration and information about the system, interfaces, chassis, routing protocols, routing tables, routing policy filters, and other features.
- **Configuring**—View the current configurations at a glance, configure the routing platform, and manage configuration files. The J-Web interface provides the following different configuration methods:
 - Configure the routing platform quickly and easily without configuring each statement individually.
 - Edit a graphical version of the Junos OS CLI configuration statements and hierarchy.
 - Edit the configuration in a text file.
 - Upload a configuration file.

The J-Web interface also allows you to manage configuration history and set a rescue configuration.

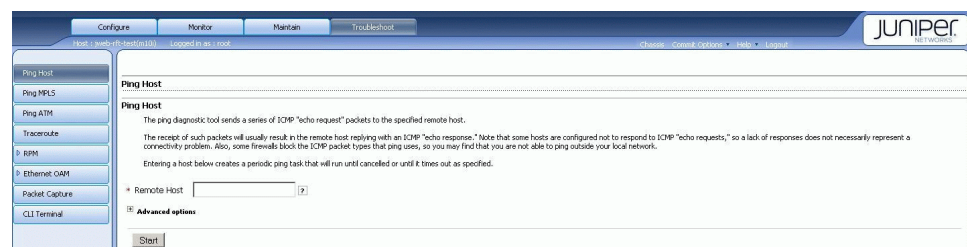
- Troubleshooting—Troubleshoot routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic.
- Maintaining—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms. On J Series routers, you can also manage software packages and licenses and copy a snapshot of the system software to a backup device.
- Configuring and monitoring events—Filter and view system log messages that record events occurring on the router. You can configure files to log system log messages and also assign attributes, such as severity levels, to messages.
- Configuring and monitoring alarms—On J Series routers only, monitor and diagnose the router by monitoring active alarms that alert you to the conditions on a network interface. You can also set the conditions that trigger alarms on an interface.

J-Web Layout

Each page of the J-Web interface is divided into the following panes, as shown in [Figure 1 on page 4](#).

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, troubleshoot, and manage the routing platform by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays subtasks of the Configure, Monitor, Maintain, or Troubleshoot task currently displayed in the main pane. For the configuration editor, this pane displays the hierarchy of configuration statements committed on the router. Click an item to access it in the main pane.

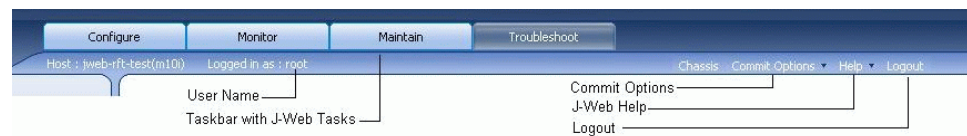
Figure 1: J-Web Layout



Top Pane Elements

The top pane comprises the elements shown in [Figure 2 on page 5](#).

Figure 2: Top Pane Elements



- *hostname – model*—Hostname and model of the routing platform.
- Logged in as: *username*—Username you used to log in to the routing platform.
- Commit Options
 - Commit—Commits the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be committed.
 - Compare—Displays the differences between the committed and uncommitted configuration on the device.
 - Discard—Discards the candidate configuration. Changes made by other users as well as changes made in other J-Web sessions will be discarded.
 - Preference—Enables you to select preferences for committing configuration. **Commit Check** only validates the configuration and reports errors. **Commit** validates and commits the configuration specified on every J-Web page.
- Help
 - Help Contents—Link to context-sensitive help information.
 - About—Link to information about the J-Web interface, such as the version number.
- Logout—Ends your current login session with the routing platform and returns you to the login page.
- Taskbar—Menu of J-Web tasks. Click a J-Web task to access it.
 - **Configure**—Configure the routing platform by using Configuration pages or the configuration editor, and view configuration history.
 - **Monitor**—View information about configuration and hardware on the routing platform.
 - **Maintain**—Manage files and licenses, upgrade software, and reboot the routing platform.
 - **Troubleshoot**—Troubleshoot network connectivity problems.

Main Pane Elements

The main pane comprises the elements shown in [Figure 3 on page 6](#).

Figure 3: Main Pane Elements

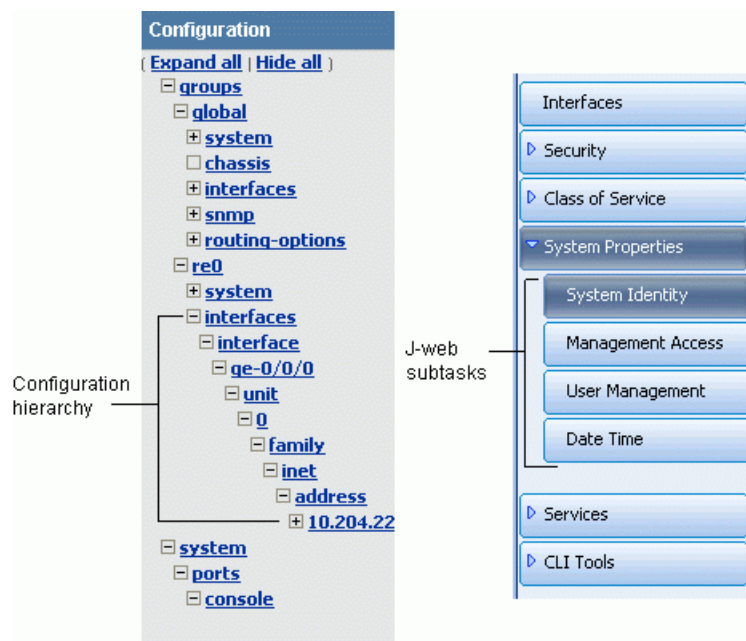
The screenshot shows the 'Configure' tab for 'SNMP'. Under the 'Traps' section, there is a 'Trap Group Name' field with a red asterisk indicating it is required. Below this are checkboxes for various categories: Authentication, Chassis, Configuration, Link, Remote operations, RMON alarm, Routing, Startup, and VRRP events. A 'Targets' field is present with a help icon (?) and a tooltip that reads: 'Targets: The value should be: A host name or IP Address'. At the bottom of the form are 'Add', 'Delete', 'OK', and 'Cancel' buttons.

- Help (?) icon—Displays useful information when you move the cursor over the question mark. This help displays field-specific information, such as the definition, format, and valid range of the field.
- Red asterisk (*)—Indicates a required field.
- Icon Legend— For the Edit Configuration subtask (J-Web configuration editor) only, explains icons that appear in the user interface to provide information about configuration statements:
 - C—Comment. Move your cursor over the icon to view a comment about the configuration statement.
 - I—Inactive. The configuration statement does not affect the routing platform.
 - M—Modified. The configuration statement is added or modified.
 - *—Mandatory. The configuration statement must have a value.

Side Pane Elements

The side pane comprises the elements shown in [Figure 4 on page 7](#).

Figure 4: Side Pane Elements



- Subtask—Displays options related to the selected task in the J-Web taskbar.
- Configuration hierarchy—For the J-Web configuration editor, displays the hierarchy of committed statements in the routing platform configuration.
 - Click **Expand all** to display the entire hierarchy.
 - Click **Hide all** to display only the statements at the top level.
 - Click plus signs (+) to expand individual items.
 - Click minus signs (–) to hide individual items.

Navigating the J-Web Interface

The layout of the panes allows you to quickly navigate through the interface. You navigate the J-Web interface, move forward and backward, scroll pages, and expand and collapse elements as you do in a typical Web browser interface.

From the taskbar, select the J-Web task that you want to perform. Selecting the task displays related subtasks in the side pane. When you select a subtask, related fields are displayed in the main pane. By default, the system selects the first subtask and displays its related fields in the main pane. The side pane and taskbar are available from all pages, allowing you to skip from one task or subtask to the other from any page in the interface.

You can easily navigate to most subtasks by selecting them from the side pane. On pages where you are required to take an action, buttons and links allow you to move to the next or previous page as you perform certain actions. For more information, see [“Navigating the J-Web Configuration Editor” on page 8](#).

Navigating the J-Web Configuration Editor

When you select **Configure>CLI Tools>Point and Click CLI** (J-Web configuration editor), the side pane displays the top level of the configured hierarchy committed on the routing platform. The main pane displays the configuration hierarchy options.

You can click a statement or identifier displayed in the main pane, or in the hierarchy in the left pane, to display the corresponding configuration options in the main pane. For more information, see [“Point and Click CLI \(J-Web Configuration Editor\)” on page 25](#).

After typing or selecting your configuration edits, click a button in the main pane (described in [Table 3 on page 8](#)) to move to the previous page after applying or committing the configuration. An updated configuration does not take effect until you commit it.

Table 3: Key J-Web Edit Configuration Buttons

Function	Button
Apply edits to the candidate configuration, and return one level up (previous page) in the configuration hierarchy.	OK
Clear the entries you have not yet applied to the candidate configuration, and return one level up (previous page) in the configuration hierarchy.	Cancel
Verify edits and apply them to the current configuration file running on the routing platform. For more details, see “Committing a Configuration” on page 39 .	Commit
Discard changes or delete configuration.	Discard

Getting J-Web Help

The J-Web interface provides two ways to display Help for the Monitor, Configure, Troubleshoot, and Maintain tasks.

To get Help in the J-Web interface:

- **Field-sensitive Help**—Move the cursor over the question mark (?) next to the field for which you want more information. The system displays useful information about the field. Typically, this Help includes one line of information about what this field does or what you must enter in a given text box. For example, Help for the Peer Autonomous System Number field states, “the value should be a number between 1 and 65535.”
- **Context-sensitive Help**—Click **Help** in the taskbar to open a separate page displaying the summary of all the fields on that page. To exit Help, close the page. You can navigate Help pages using hypertext links connecting related topics, or click the following options (if available) at the top and bottom of each page. [Figure 5 on page 9](#) shows Help for the CoS Configuration page.
 - **Prev**—Access the previous page.
 - **Next**—Access the next page.

- **Report an Error**—Access a form for providing feedback.

Figure 5: CoS Help Page

[\[Next\]](#)[\[Report an Error\]](#)

Configuring a Stateless Firewall Filter with Quick Configuration

The Firewall Filters Quick Configuration pages allow you to configure stateless firewall filters that examine packets traveling to or from a routing platform. You can create new filters or edit existing filters by adding terms to them. Each filter term is defined by a set of match conditions and an associated action. After you define the terms for a filter, you must associate the filter with one or more interfaces on the router.

This section contains the following topics:

- [Configuring IPv4 and IPv6 Stateless Firewall Filters](#)
- [Assigning IPv4 and IPv6 Firewall Filters to Interfaces](#)

[\[Next\]](#)[\[Report an Error\]](#)

Copyright © 2009, Juniper Networks, Inc. [All rights reserved. Trademark Notice.](#)

CHAPTER 2

Installation and Setup

- [J-Web Software Requirements on page 11](#)
- [Installing the J-Web Software on page 11](#)
- [Starting the J-Web Interface on page 12](#)
- [Configuring Basic Settings on page 14](#)

J-Web Software Requirements

To access the J-Web interface for all platforms, your management device requires the following software:

- Supported browsers— Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0
- Language support— English-version browsers
- Supported OS— Microsoft Windows XP Service Pack 3

Other browser versions might not provide access to the J-Web interface.

Installing the J-Web Software

Your routing platform comes with the Junos OS installed on it. When you power on the routing platform, all software starts automatically. On J Series routers, the J-Web software is part of the Junos OS available by default. However, on M Series and T Series routers, you need to install the J-Web software because it is not shipped on the routing platform.

If your routing platform is not shipped with the J-Web software on it, you must download the J-Web software package from the Juniper Networks webpage and install it on your routing platform. After the installation, you must enable Web management of the routing platform with the CLI.



NOTE: M Series or T Series routers must be running Junos OS version 7.3 or later to support the J-Web interface.

To install and enable the J-Web software:

1. Using a Web browser, navigate to the Juniper Networks Customer Support Center at <https://www.juniper.net/customers/csc/software/>.
2. Log in to the Juniper Networks authentication system with the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Download the J-Web software to your local host. Select the version that is the same as the Junos OS version running on the routing platform.
4. Copy the software package to the routing platform. We recommend that you copy it to the `/var/tmp` directory.
5. If you have previously installed the J-Web software on the routing platform, you must delete it before installing the new version. To do so, from operational mode in the CLI, enter the following command:

```
user@host> request system software delete jweb
```

6. Install the new package on the routing platform. From operational mode in the CLI, enter the following command:

```
user@host> request system software add path/filename
```

Replace *path* with the full pathname to the J-Web software package. Replace *filename* with the filename of the J-Web software package.

7. Enable Web management of the routing platform. From configuration mode in the CLI, enter the following command:

```
user@host# system services web-management http
```

Starting the J-Web Interface

Before you start the user interface, you must perform the initial routing platform configuration described in the routing platform hardware guide. After the initial configuration, you use your username and password and the hostname or IP address of the router to start the user interface.

To start the J-Web interface:

1. Launch a Web browser that has Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the Junos OS. To use HTTPS, you must have installed a certificate on the routing platform and enabled HTTPS.



NOTE: If the routing platform is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the routing platform.

2. After **http://** or **https://** in your Web browser, type the hostname or IP address of the routing platform, and press Enter.

The J-Web login page appears.

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

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



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

The J-Web **Initial Configuration Set Up** page appears.

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

Configuring Basic Settings

Before you begin initial configuration, complete the following tasks:

- Install the routing platform in its permanent location, as described in the hardware installation guide or the Getting Started Guide for your routing platform.
- Gather the following information:
 - Hostname for the router on the network
 - Domain that the router belongs to on the network
 - Password for the root user
 - Time zone where the router is located
 - IP address of a Network Time Protocol (NTP) server (if NTP is used to set the time on the router)
 - IP address of a Domain Name System (DNS) server
 - List of domains that can be appended to hostnames for DNS resolution
 - IP address of the default gateway
 - IP address to be used for the loopback interface
 - IP address of the built-in Ethernet interface that you will use for management purposes
- Collect the following equipment:
 - A management device, such as a laptop, with an Ethernet port
 - An Ethernet cable

To configure basic settings with J-Web Initial Configuration:

1. Enter information into the Initial Configuration Set Up page (see [Figure 6 on page 15](#)), as described in [Table 4 on page 15](#).
2. Click **Apply** to apply the configuration.

Figure 6: J-Web Set Up Initial Configuration Page

Initial Configuration

Set Up

Identification

* Host Name: ?

Domain Name: ?

* Root Password: ?

* Verify Root Password: ?

Time

Time Zone: ?

NTP Servers: ?

Current System Time: ?

?

?

Network

DNS Name Servers: ?

Domain Search: ?

Default Gateway:

Loopback Address: ?

fe-0/0/0.0 Address:

Management Access

The following access methods are considered insecure as any information sent over them will be sent without encryption and could possibly be intercepted during transmission.

Allow Telnet Access: ☒

Allow JUNOScript over Clear-Text Access: ☐

The following access method is considered secure as any information sent over it will be encrypted before transmission.

Allow SSH Access: ☒

In order to enable HTTPS or JUNOScript over SSL, you will need to visit the SSL configuration page to configure certificates and associations.



NOTE: For J Series routers only, after initial configuration is complete, the routing platform stops functioning as a Dynamic Host Configuration Protocol (DHCP) server. If you change the IP address of the management interface and have the management device configured to use DHCP, you lose your DHCP lease and your connection to the routing platform through the J-Web interface. To reestablish a connection, either set the IP address on the management device manually, or connect the management interface to the management network and access the routing platform another way—for example, through the console port.

Table 4: Initial Configuration Set Up Summary

Field	Function	Your Action
Identification		
Host Name (required)	Defines the hostname of the router.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password (required)	Sets the root password that the user “root” can use to log in to the router.	Type a plain-text password that the system encrypts. NOTE: After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.

Table 4: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
Verify Root Password (required)	Verifies that the root password has been typed correctly.	Retype the password.
Time		
Time Zone	Identifies the time zone that the router is located in.	From the list, select the appropriate time zone.
NTP Servers	Specify an NTP server that the router can reach to synchronize the system time.	<p>To add an IP address, type it in the box to the left of the Add button, then click Add.</p> <p>To delete an IP address, click it in the box above the Add button, then click Delete.</p>
Current System Time	Synchronizes the system time with the NTP server, or manually sets the system time and date.	<ul style="list-style-type: none"> To immediately set the time using the NTP server, click Set Time via NTP. The router sends a request to the NTP server and synchronizes the system time. <p>NOTE: If you are configuring other settings on this page, the router also synchronizes the system time using the NTP server when you click Apply.</p> <ul style="list-style-type: none"> To set the time manually, click Set Time Manually. A pop-up window allows you to select the current date and time from lists.
Network		
DNS Name Servers	Specify a DNS server that the router can use to resolve hostnames into addresses.	<p>To add an IP address, type it in the box to the left of the Add button, then click Add.</p> <p>To delete an IP address, click it in the box above the Add button, then click Delete.</p>
Domain Search	Adds each domain name that the router is included in to the configuration so that they are included in a DNS search.	<p>To add a domain name, type it in the box to the left of the Add button, then click Add.</p> <p>To delete a domain name, click it in the box above the Add button, then click Delete.</p>
Default Gateway	Defines a default gateway through which to direct packets addressed to networks not explicitly listed in the routing table.	Type a 32-bit IP address, in dotted decimal notation.
Loopback Address	Defines a reserved IP address that is always available on the router. If no address is entered, this address is set to 127.0.0.1/32.	Type a 32-bit IP address and prefix length, in dotted decimal notation.

Table 4: Initial Configuration Set Up Summary (*continued*)

Field	Function	Your Action
fe-0/0/0 Address (on J2300, J4300, and J6300 routers)	Defines the IP address and prefix length of the management interface. The management interface is used for accessing the router. The DHCP client sets this address to 192.168.1.1/24 if no DHCP server is found.	Type a 32-bit IP address and prefix length, in dotted decimal notation.
ge-0/0/0 Address (on J4350 and J6350 routers)		NOTE: You must enter the address for the management interface on the Quick Configuration Set Up page before you click Apply . If you do not manually configure this address, you will lose your connection to the J-Web interface when you click Apply .
fxp0 Address (on M Series routers)		
Management Access		
Allow Telnet Access	Allows remote access to the router by using Telnet.	To enable Telnet access, select the check box.
Allow JUNOScript protocol over Clear-Text Access	Allows JUNOScript to access the router by using a protocol for sending unencrypted text over a TCP connection.	To enable JUNOScript access over clear text, select the check box.
Allow SSH Access	Allows remote access to the router by using SSH.	To enable SSH access, select the check box.

CHAPTER 3

Secure Web Access

- [Secure Web Access Overview on page 19](#)
- [Generating SSL Certificates on page 19](#)

Secure Web Access Overview

A routing platform uses the Secure Sockets Layer (SSL) protocol to provide secure management of routing platforms through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for the SSL service. SSL encrypts communication between your routing platform and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the routing platform through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you are not able to access the routing platform through HTTPS.

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

On J Series routers, HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

Generating SSL Certificates

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

To generate an SSL certificate:

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

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

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

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

cat new.pem

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

Go on to [“Configuring Secure Web Access” on page 47](#) to install the SSL certificate and enable HTTPS.

PART 2

Configuration

- [Configuration Tools on page 23](#)
- [Configuration Tasks on page 35](#)

CHAPTER 4

Configuration Tools

- [Configuration Task Overview on page 23](#)
- [Point and Click CLI \(J-Web Configuration Editor\) on page 25](#)
- [CLI Viewer \(View Configuration Text\) on page 28](#)
- [CLI Editor \(Edit Configuration Text\) on page 29](#)
- [CLI Terminal Requirements on page 30](#)
- [Starting the CLI Terminal on page 31](#)
- [Using the CLI Terminal on page 32](#)

Configuration Task Overview

The J-Web user interface provides different methods for configuring your routing platform with the Junos OS. Choose a configuration method appropriate to your needs and familiarity with the interface.

Use the J-Web user interface to configure the services supported on a routing platform, including system settings, routing protocols, interfaces, network management, and user access.

Alternatively, you can configure the routing platform services with the Junos OS command-line interface (CLI) from a console connection to the routing platform or a remote network connection. You can also access the CLI from the J-Web interface. For more information, see [“Using the CLI Terminal” on page 32](#). For complete information about using the CLI, see the *Junos OS CLI User Guide*.

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, but do not take effect on the routing platform until you *commit* the changes.

You can set your preference by selecting **Commit** or **Commit Check**. This preference is applicable across sessions and users. **Commit Check** only validates the configuration and reports errors. **Commit** validates and commits the configuration specified on every J-Web page.

When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple

users are editing the configuration when you commit the candidate configuration, all changes made by all the users take effect. If you are editing the configuration with the CLI, you can edit an *exclusive* or *private* candidate configuration. For more information, see the [Junos OS CLI User Guide](#).

When you commit a configuration, the routing platform saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49. You can roll back the configuration to any saved version.



NOTE: You must assign a root password before committing a configuration and can do so on the J-Web Set Up page.

To better understand the Junos OS configuration process, become familiar with the terms defined in [Table 5 on page 24](#).

Table 5: Junos OS Configuration Terms

Term	Definition
candidate configuration	A working copy of the configuration that can be edited without affecting the routing platform until it is committed.
configuration group	Group of configuration statements that can be inherited by the rest of the configuration.
commit a configuration	Have the candidate configuration checked for proper syntax, activated, and marked as the current configuration file running on the routing platform.
configuration hierarchy	Set of hierarchically organized configuration statements that make up the Junos [®] OS configuration on a routing platform. There are two types of statements: <i>container statements</i> , which contain other statements, and <i>leaf statements</i> , which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.
rescue configuration	On J Series routers only, a configuration that recovers a routing platform from a configuration that denies management access. You set a current committed configuration through the J-Web interface or CLI for emergency use. To load and commit the rescue configuration, you press and release the CONFIG or RESET CONFIG button.
roll back a configuration	Return to a previously committed configuration.

Point and Click CLI (J-Web Configuration Editor)

Using Point and Click CLI, you can configure all properties of the Junos OS, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

The configuration is stored as a hierarchy of statements. You create the specific hierarchy of configuration statements that you want to use. After you finish entering the configuration statements, you commit them to activate the configuration on the routing platform.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the routing platform and then committed. Edit Configuration (J-Web configuration editor) allows you to create the hierarchy interactively, and Edit Configuration Text allows you to create and commit statements as an ASCII text file.

To access Edit Configuration, also called the J-Web configuration editor, select **Configure>CLI Tools>Point and Click**. This page allows you to configure all routing platform services that you can configure from the Junos OS CLI. Each field in the J-Web configuration editor has the same name as the corresponding configuration statement at the same hierarchy level in the CLI. For example, the Policy Options field corresponds to the **policy-options** statement in the CLI. As a result, you can easily switch from one interface to the other or follow a CLI configuration example using the J-Web configuration editor.

Table 6 on page 25 lists key J-Web configuration editor tasks and their functions.

Table 6: J-Web Configuration Editor Tasks Summary

J-Web Configuration Editor Task	Function
Access	Configure network access. For example, you can configure the Point-to-Point Protocol (PPP), the tracing access processes, the Layer 2 Tunneling Protocol (L2TP), RADIUS authentication for L2TP, and Internet Key Exchange (IKE) access profiles. For more information, see the Junos OS System Basics Configuration Guide .
Accounting options	Configure accounting profiles. An accounting profile represents common characteristics of collected accounting data, including collection interval, accounting data files, and counter names on which to collect statistics. On the Accounting options pages, you can configure multiple accounting profiles, such as the interface, filter, MIB, routing engine, and class usage profiles. For more information, see the Junos OS Network Management Configuration Guide .
Applications	Define applications by protocol characteristics and group the applications you have defined into a set. On the Applications pages, you can configure application properties, such as Internet Control Message Protocol (ICMP) code and type. You can also specify application protocols—also known as application-level gateways (ALGs)—to be included in an application set for service processing, or specify network protocols to match in an application definition. For more information, see the Junos OS Services Interfaces Configuration Guide .

Table 6: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
Chassis	Configure routing platform chassis properties. On the Chassis pages, you can configure different properties of the routing platform chassis, including conditions that activate the red and yellow alarm LEDs on the routing platforms and SONET/SDH framing and concatenation properties for individual Physical Interface Cards (PICs). For more information, see the Junos OS System Basics Configuration Guide .
Class of service	Define class-of-service (CoS) components, such as CoS value aliases, classifiers, forwarding classes, rewrite rules, schedulers, and virtual channel groups. The Class of service pages also allow you to assign CoS components to interfaces. For more information, see the Junos OS Class of Service Configuration Guide .
Diameter	Configure Diameter base protocol. For example, you can specify the remote peers, the endpoint origin attributes, and network elements that associate routes with peers. For more information, see the Junos OS Subscriber Access Configuration Guide .
Event options	Configure event policies. An event policy is an if-then-else construct that defines actions to be executed by the software on receipt of a system log message. For each policy, you can configure multiple actions, as follows—ignore the event, upload a file to a specified destination, execute Junos OS operational mode commands, or execute Junos OS event scripts (op scripts). For more information, see the Junos OS Configuration and Operations Automation Guide .
Firewall	Configure stateless firewall filters. With stateless firewall filters—also known as ACLs—you can control packets transiting the routing platform to a network destination and packets destined for and sent by the routing platform. On the Firewall pages, you can create filters and add terms to them. For each term, you can set the match conditions and associate actions to be performed on packets matching these conditions. For more information, see the Junos OS Policy Framework Configuration Guide .
Forwarding options	<p>Configure traffic forwarding and traffic sampling options. You can sample IP traffic based on particular input interfaces and various fields in the packet header. You can also use traffic sampling to monitor any combination of specific logical interfaces, specific protocols on one or more interfaces, a range of addresses on a logical interface, or individual IP addresses.</p> <p>Traffic forwarding policies allow you to control the per-flow load balancing, port mirroring, and Domain Name System (DNS) or Trivial File Transfer Protocol (TFTP) forwarding. For more information, see the Junos OS Policy Framework Configuration Guide.</p>
Interfaces	Configure physical and logical interface properties. For the physical interface on the routing platform, you can modify default values for general interface properties, such as the interface's maximum transmission unit (MTU) size, link operational mode, and clock source. For each logical interface, you can specify the protocol family and other logical interface properties. For more information, see the Junos OS Network Interfaces Configuration Guide .
Jsrc	Configure Jsrc. For example, you can configure the JSRC partition, associate a Diameter instance, SAE hostname, and the SAE realm with the partition. For more information, see the Junos OS Subscriber Access Configuration Guide .
Policy options	Configure policies by specifying match conditions and associating actions with the conditions. On the Policy options page, you can create a named community and define autonomous system (AS) paths, damping parameters, and routing policies. You can also create a named prefix list and include it in a routing policy. For more information, see the Junos OS VPNs Configuration Guide .

Table 6: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
Protocols	Configure routing protocols such as Border Gateway Protocol (BGP), Distance Vector Multicast Routing Protocol (DVMRP), Intermediate System-to-Intermediate System (IS-IS), Multiprotocol Label Switching (MPLS), Open Shortest Path First (OSPF), Resource Reservation Protocol (RSVP) and Routing Information Protocol (RIP). For more information, see the Junos OS Routing Protocols Configuration Guide and the Junos OS MPLS Applications Configuration Guide .
Routing instances	Configure routing instances. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. On the Routing instances pages, you can configure the following types of routing instances: forwarding, Layer 2 virtual private network (VPN), nonforwarding, VPN routing and forwarding (VRF), virtual router, and virtual private LAN service (VPLS). For more information, see the Junos OS Routing Protocols Configuration Guide .
Routing options	<p>Configure protocol-independent routing options that affect systemwide routing operations. On the Routing options pages, you can perform the following tasks:</p> <ul style="list-style-type: none"> • Add routing table entries, including static routes, aggregated (coalesced) routes, generated routes (routes of last resort), and martian routes (routes to ignore). • Create additional routing tables and routing table groups. • Set the AS number of the routing platform for use by BGP. • Set the router ID, which is used by BGP and OSPF to identify the routing platform from which a packet originated. • Define BGP confederation members for use by BGP. • Configure how much system logging information to log for the routing protocol process. • Configure systemwide tracing (debugging) to track standard and unusual routing operations and record this information in a log file. <p>For more information, see the Junos OS Routing Protocols Configuration Guide.</p>
Security	Configure Internet Protocol Security (IPsec) for authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, you can configure the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). You can also configure the SSH known host list, and the trace options for IPsec key management. For more information, see the Junos OS System Basics Configuration Guide .
Services	Configure application settings for services interfaces, such as dynamic flow capture parameters, the intrusion detection service (IDS), IPsec VPN service, RPM, stateful firewalls, and Network Address Translation (NAT). For more information, see the Junos OS Services Interfaces Configuration Guide .
Snmp	Configure SNMP to monitor network devices from a central location. You can specify an administrative contact and location and add a description for each system being managed by SNMP. You can also configure SNMP community strings, trap options, and interfaces on which SNMP requests can be accepted. For more information, see the Junos OS Network Management Configuration Guide .
System	Configure system management functions, including the router's hostname, address, and domain name; the addresses of Domain Name System (DNS) servers; user login accounts, including user authentication and the root-level user account; time zones and Network Time Protocol (NTP) properties; and properties of the router's auxiliary and console ports. For more information, see the Junos OS System Basics Configuration Guide .

CLI Viewer (View Configuration Text)

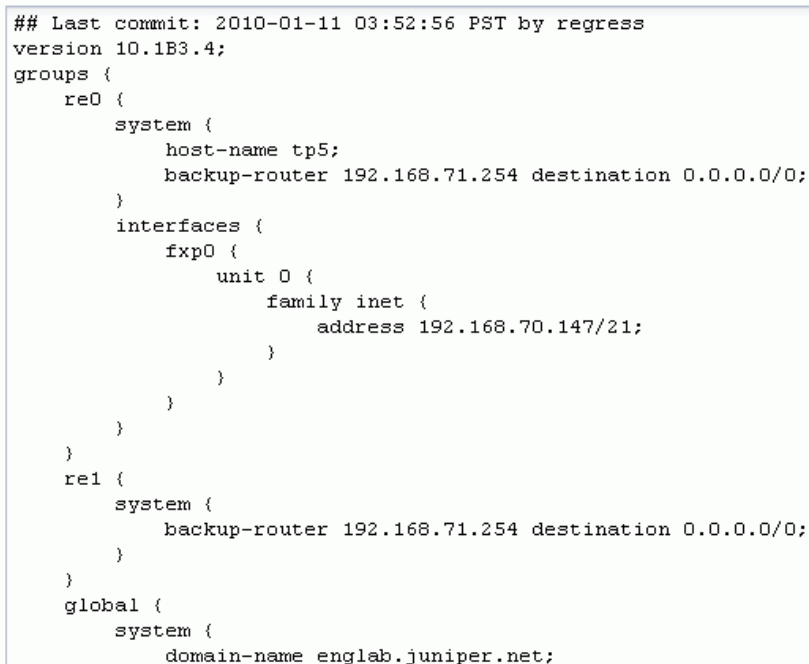
To view the entire configuration in text format, select **Configure>CLI Tools>CLI Viewer**. The main pane displays the configuration in text format (see [Figure 7 on page 28](#)). The displayed configuration is the same as the configuration displayed when you enter the Junos OS CLI command **show configuration**.

Figure 7: View Configuration Text Page

CLI Viewer

The CLI Viewer page shows the current configuration running on the device.

The current configuration running on the device is



```
## Last commit: 2010-01-11 03:52:56 PST by regress
version 10.1B3.4;
groups {
  re0 {
    system {
      host-name tp5;
      backup-router 192.168.71.254 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.70.147/21;
          }
        }
      }
    }
  }
  re1 {
    system {
      backup-router 192.168.71.254 destination 0.0.0.0/0;
    }
  }
  global {
    system {
      domain-name englab.juniper.net;
    }
  }
}
```

The configuration statements appear in a fixed order, irrespective of the order in which you configured the routing platform. The top of the configuration displays a timestamp indicating when the configuration was last changed and the current version. [Figure 7 on page 28](#) shows that user **regress** committed the last configuration on 11 January 2010, and the software version running on the routing platform is Junos OS Release 10.1.

Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, using an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon (;), as does the last statement in the hierarchy.

This indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is

not so strict. The braces and semicolons are required, but the indentation and use of new lines are not required in ASCII configuration files.

CLI Editor (Edit Configuration Text)

Using View and Edit, you can configure all properties of the Junos OS, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

The configuration is stored as a hierarchy of statements. You create the specific hierarchy of configuration statements that you want to use. After you finish entering the configuration statements, you commit them to activate the configuration on the routing platform.

You can create the hierarchy interactively, or you can create an ASCII text file that is loaded onto the routing platform and then committed. Edit Configuration (J-Web configuration editor) allows you to create the hierarchy interactively, and Edit Configuration Text allows you to create and commit statements as an ASCII text file.

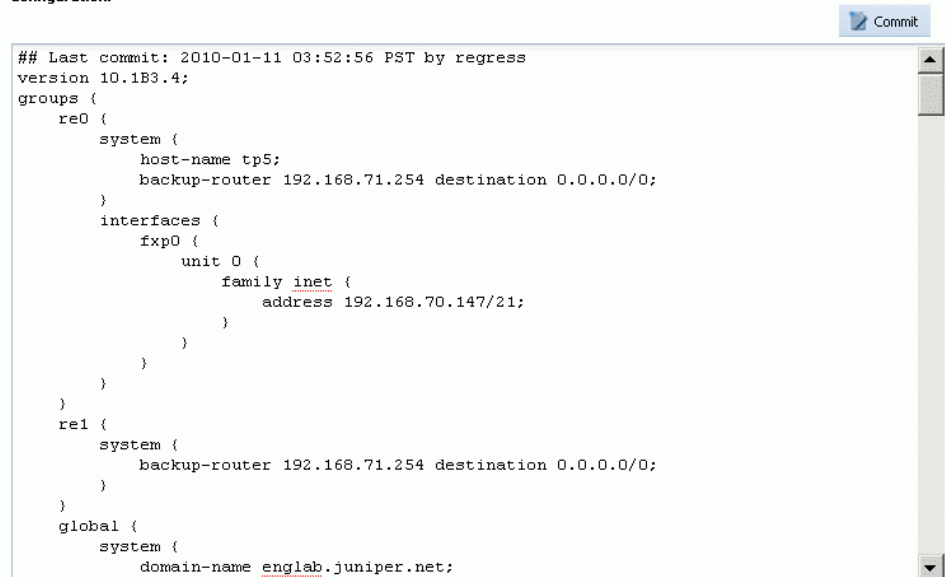
To edit the entire configuration in text format, select **Configure>CLI Tools>CLI Editor**. The main pane displays the configuration in a text editor (see [Figure 8 on page 29](#)).

Figure 8: Edit Configuration Text Page

CLIEditor

Edit the configuration. When you click "Commit", the edited configuration replaces the existing configuration and takes effect. If any errors occur when the configuration is loading or committed, they are displayed and the previous configuration is restored.

Configuration:



```
## Last commit: 2010-01-11 03:52:56 PST by regress
version 10.1B3.4;
groups {
  re0 {
    system {
      host-name tp5;
      backup-router 192.168.71.254 destination 0.0.0.0/0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.70.147/21;
          }
        }
      }
    }
  }
  re1 {
    system {
      backup-router 192.168.71.254 destination 0.0.0.0/0;
    }
  }
  global {
    system {
      domain-name englab.juniper.net;
    }
  }
}
```

For more information about the format of an ASCII configuration file, see “[CLI Viewer \(View Configuration Text\)](#)” on page 28.



CAUTION: We recommend that you use this method to edit and commit the configuration only if you have experience editing configurations through the CLI.

To edit the entire configuration in text format:

1. Navigate to the hierarchy level you want to edit.
2. Edit the candidate configuration using standard text editor operations—insert lines (with the Enter key), delete lines, and modify, copy, and paste text.
3. Click **Commit** to load and commit the configuration.

The routing platform checks the configuration for the correct syntax before committing it.

When you edit the ASCII configuration file, you can add comments of one or more lines. Comments must precede the statement they are associated with. If you place the comments in other places in the file, such as on the same line after a statement or on a separate line following a statement, they are removed when you click Commit. Comments must begin and end with special characters. For more information, see the *Junos OS CLI User Guide*.

CLI Terminal Requirements

To access the CLI through the J-Web interface, your management device requires the following features:

- SSH access—Enable SSH on your system. SSH provides a secured method of logging in to the routing platform, to encrypt traffic so that it is not intercepted. If SSH is not enabled on the system, the CLI terminal page displays an error and provides a link to the Set Up Quick Configuration page that allows you to enable SSH. For more information, see “[Configuring Basic Settings](#)” on page 14.
- Java applet support—Make sure that your Web browser supports Java applets.
- JRE installed on the client—Install Java Runtime Environment (JRE) version 1.4 or later on your system. JRE is a software package that must be installed on a system to run Java applications. Download the latest JRE version from the Java Software website <http://www.java.com/>. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.



NOTE: The CLI terminal is supported on JRE version 1.4 and later only.

Starting the CLI Terminal

To get started on the CLI terminal:

1. Make sure that your system meets the requirements mentioned in [“CLI Terminal Requirements” on page 30](#).
2. In the J-Web interface, select **Troubleshoot>CLI Terminal**. A Java applet is downloaded into the J-Web interface allowing SSH access to the routing platform.
3. Log in to the CLI by typing your Junos OS password. This is the same password that you use to log in to the J-Web interface.

After you log in, a percentage sign (%) prompt appears to indicate that you are in the UNIX shell (see [Figure 9 on page 32](#)).

4. To start the CLI, type **cli**.

The presence of the angle bracket (>) prompt indicates that the CLI has started. By default, the prompt is preceded by a string that contains your username and the hostname of the routing platform. The angle bracket also indicates that you are in operational mode.

5. To enter configuration mode, type **configure**. The **[edit]** prompt indicates the current configuration mode.
6. Type **exit** or **quit** to return to the previous level of the configuration—for example, to return to operational mode from configuration mode.

For security purposes, each time you log out of the routing platform or leave the CLI terminal page, the CLI terminal session ends and you are required to reenter your password. When you select **Troubleshoot>CLI Terminal** again, retype your Junos OS password to access the CLI.

Figure 9: Starting the CLI Terminal**CLI Terminal**

A Java applet will be loaded below that will provide an SSH connection between your browser and '10.209.8.129'. You will be asked to enter your password again as a security measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

```
root@betsy% cli
root@betsy> configure
Entering configuration mode

[edit]
root@betsy# exit
Exiting configuration mode

root@betsy> quit

root@betsy% █
```

Using the CLI Terminal

The Junos OS CLI uses industry-standard tools and utilities to provide a set of commands for monitoring and configuring a routing platform. You type commands on a line and press Enter to execute them. The CLI provides command help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The J-Web CLI terminal provides access to the Junos OS CLI through the J-Web interface. The functionality and behavior of the CLI available through the CLI terminal page is the same as the Junos OS CLI available through the routing platform console. The CLI terminal supports all CLI commands and other features such as CLI help and autocompletion. Using the CLI terminal page, you can fully configure, monitor, and manage your routing platform.

The commands in the CLI are organized hierarchically, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the routing platform system and system software are grouped under the **show** command, and all commands that display information about the routing table are grouped under the **show route** command. The hierarchical organization results in commands that have a regular syntax and provides the following features that simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software they are operating on. For

example, all **show** commands display software information and statistics, and all **clear** commands erase various types of system information.

- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command.
- Command completion—Command completion for command names (keywords) and command options is also available at each level of the hierarchy. In the CLI terminal, you can do one of the following for command completions:
 - Type a partial command name followed immediately by a question mark (with no intervening space) to see a list of commands that match the partial name you typed.
 - Press the Spacebar to complete a command or option that you have partially typed. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a prompt indicates that you have entered an ambiguous command, and the possible completions are displayed.

The Tab key option is currently not available on the CLI terminal.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the routing platform, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the routing platform.

For more information about the Junos OS CLI, see the [Junos OS CLI User Guide](#). For information about configuring and monitoring Junos OS features with the CLI, see <http://www.juniper.net/books>.

[Figure 10 on page 34](#) shows the CLI terminal displaying all the options that you can configure in CLI configuration mode.

Figure 10: J-Web CLI Terminal

CLI Terminal

A Java applet will be loaded below that will provide an SSH connection between your browser and '10.209.8.129'. You will be asked to enter your password again as a security measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

```
root@betsy# set ?
Possible completions:
> access                Network access configuration
> access-profile        Access profile for this instance
> accounting-options     Accounting data configuration
> applications          Define applications by protocol characteristics
+ apply-groups          Groups from which to inherit configuration data
> chassis              Chassis configuration
> class-of-service      Class-of-service configuration
> event-options          Event processing configuration
> firewall              Define a firewall configuration
> forwarding-options    Configure options to control packet forwarding
> groups                Configuration groups
> interfaces            Interface configuration
> policy-options        Routing policy option configuration
> protocols             Routing protocol configuration
> routing-instances     Routing instance configuration
> routing-options       Protocol-independent routing option configuration
> security              Security configuration
> services
> snmp                  Simple Network Management Protocol configuration
> system                System parameters
[edit]
root@betsy#
```

CHAPTER 5

Configuration Tasks

- [Editing and Committing a Junos OS Configuration on page 35](#)
- [J-Web Configuration Tasks on page 35](#)
- [Editing a Configuration on page 36](#)
- [Committing a Configuration on page 39](#)
- [Discarding Parts of a Candidate Configuration on page 39](#)
- [Accounting Options on page 40](#)

Editing and Committing a Junos OS Configuration

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, but do not take effect on the routing platform until you *commit* the changes.

When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, all changes made by all the users take effect. If you are editing the configuration with the CLI, you can edit an *exclusive* or *private* candidate configuration. For more information, see the [Junos OS CLI User Guide](#).

When you commit a configuration, the routing platform saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49. You can roll back the configuration to any saved version.



NOTE: You must assign a root password before committing a configuration and can do so on the J-Web Set Up page.

J-Web Configuration Tasks

J-Web configuration pages offer you several different ways to configure your routing platform. Configuration pages provide access to all the configuration statements

supported by the routing platform, so you can fully configure it without using the CLI. You can also manage the configuration, monitor user access, and set a rescue configuration.

[Table 7 on page 36](#) provides a summary of the J-Web configuration tasks.

Table 7: J-Web Configuration Tasks Summary

J-Web Configuration Task	Description	More Information
Edit the configuration using a clickable interface	Expand the entire configuration hierarchy in the side pane and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option.	“Point and Click CLI (J-Web Configuration Editor)” on page 25
Edit the configuration in text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	“CLI Editor (Edit Configuration Text)” on page 29
Upload a configuration file	Upload a complete configuration.	“Upload Configuration File” on page 90
View the configuration in text format	View the entire configuration on the routing platform in text format.	“CLI Viewer (View Configuration Text)” on page 28

Editing a Configuration

To edit the configuration on a series of pages of clickable options that step you through the hierarchy, select **Configure>CLI Tools>Point and Click**. The side pane displays the top level of the configuration hierarchy, and the main pane displays configured hierarchy options and the Icon Legend (see [Figure 11 on page 37](#)).

Figure 11: Edit Configuration Page

Configuration

Expand all | Hide all |

- groups
- system

Refresh Commit... Discard...

Configuration

- Access [Configure](#)
- Accounting options [Configure](#)
- Applications [Configure](#)
- Chassis [Configure](#)
- Class of service [Configure](#)
- Diameter [Configure](#)
- Event options [Configure](#)
- Firewall [Configure](#)
- Forwarding options [Configure](#)
- Interfaces [Configure](#)
- Jsrc [Configure](#)
- Policy options [Configure](#)
- Protocols [Configure](#)
- Routing instances [Configure](#)
- Routing options [Configure](#)
- Security [Configure](#)
- Services [Configure](#)
- Snmp [Configure](#)
- System [Edit](#) [Delete](#)

Access profile

Access profile name ?

Jsrc partition

Jsrc partition name ?

Advanced

Apply groups [Add new entry](#)

Value	Actions
global	Edit Delete
re0	Edit Delete

Refresh Commit... Discard...

Icon Legend

- C Comment**
The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
- I Inactive**
The configuration statement is not active and does not affect the device.
- M Modified**
The configuration statement has been changed or added.
- M Mandatory**
The configuration statement must have a value.

To expand or hide the hierarchy of all the statements in the side pane, click **Expand all** or **Hide all**. To expand or hide an individual statement in the hierarchy, click the expand (+) or collapse (–) icon to the left of the statement.



NOTE: Only those statements included in the committed configuration are displayed in the side pane hierarchy.

The configuration information in the main pane consists of configuration options that correspond to configuration statements. Configuration options that contain subordinate statements are identified by the term *nested configuration*.

To include, edit, or delete statements in the candidate configuration, click one of the links described in [Table 8 on page 38](#) in the main pane. Then specify configuration information by typing into a field, selecting a value from a list, or clicking a check box (toggle).

Table 8: J-Web Edit Configuration Links

Link	Function
Add new entry	Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.
Configure	Displays information for a configuration option that has not been configured, allowing you to include a statement.
Delete	Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.
Edit	Displays information for a configuration option that has already been configured, allowing you to edit a statement.
<i>identifier</i>	Displays fields and lists for an existing statement identifier, allowing you to edit the identifier.

As you navigate through the configuration, the hierarchy level is displayed at the upper right of the main pane. You can click a statement or identifier in the hierarchy to return to the corresponding configuration options in the main pane.

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. [Table 9 on page 38](#) describes the meaning of these icons.

Table 9: J-Web Edit Configuration Icons

Icon	Meaning
C	Displays a comment about a statement.
I	Indicates that a statement is inactive.
M	Indicates that a statement has been added or modified, but has not been committed.
*	Indicates that the statement or identifier is required in the configuration.
?	Provides help information.



NOTE: You can annotate statements with comments or make them inactive only through the CLI. For more information, see the [Junos OS CLI User Guide](#).

After typing or selecting your configuration edits, click a button in the main pane (described in [Table 10 on page 39](#)) to apply your changes or refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

Table 10: J-Web Edit Configuration Buttons

Button	Function
OK	Applies edits to the candidate configuration, and returns you to the previous level in the configuration hierarchy.
Cancel	Clears the entries you have not yet applied to the candidate configuration, and returns you to the previous level in the configuration hierarchy.
Refresh	Updates the display with any changes to the configuration made by other users. .
Commit	Verifies edits and applies them to the current configuration file running on the routing platform. For details, see “Committing a Configuration” on page 39 .
Discard	Removes edits applied to, or deletes existing statements or identifiers from, the candidate configuration. For details, see “Discarding Parts of a Candidate Configuration” on page 39 .

Committing a Configuration

When you finish making changes to a candidate configuration with the J-Web configuration editor, you must commit the changes to use them in the current operational software running on the routing platform.

If another user is editing an exclusive candidate configuration with the CLI, you cannot commit a configuration until the user has committed the configuration. To display a list of users, see [“Displaying Users Editing the Configuration” on page 87](#). For more information about editing an exclusive candidate configuration, see the *Junos OS CLI User Guide*.

To commit a candidate configuration:

1. In the J-Web configuration editor, click **Commit**.

The main pane displays a summary of your changes in statement form.

2. To confirm the commit operation, click **OK**.

If multiple users are editing the configuration when you commit the candidate configuration, all changes made by all users take effect.

3. To display all the edits applied to the running configuration, click **Refresh**.

Discarding Parts of a Candidate Configuration

Before committing a candidate configuration, you can discard changes you applied or delete existing statements or identifiers.

To discard parts of a candidate configuration:

1. Navigate to the level of the hierarchy you want to edit, and click **Discard**.

The main pane displays a list of target statements based on the hierarchy level and the changes you have made.

2. Select an option button to specify the appropriate discard operation or deletion. (Not all buttons appear in all situations.)
 - **Discard Changes Below This Point**—Discards changes made to the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a discarded statement are also discarded.
 - **Discard All Changes**—Discards all changes made to the candidate configuration.
 - **Delete Configuration Below This Point**—Deletes all changes and statements in the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a deleted statement are also deleted.
3. To confirm the discard operation or deletion, click **Discard**.

The updated candidate configuration does not take effect on the routing platform until you commit it.

Accounting Options

[Figure 12 on page 41](#) shows the Accounting options configuration page. This page displays the different settings that you can configure at the accounting options hierarchy level.

On the Accounting options page, click any option to view and configure related options.

Figure 12: Accounting Options Configuration Editor Page

Configuration

Accounting options

OK Cancel Refresh Commit... Discard...

Class usage profile (None configured) [Add new entry](#)

File (None configured) [Add new entry](#)

Filter profile (None configured) [Add new entry](#)

Interface profile (None configured) [Add new entry](#)

Mib profile (None configured) [Add new entry](#)





Policy decision statistics profile (None configured) [Add new entry](#)

Routing engine profile (None configured) [Add new entry](#)

Advanced

OK Cancel Refresh Commit... Discard...

Icon Legend

-  **Comment**
The configuration statement has been annotated with a comment. To display the comment, place the cursor over the statement icon.
-  **Inactive**
The configuration statement is not active and does not affect the device.
-  **Modified**
The configuration statement has been changed or added.
-  **Mandatory**
The configuration statement must have a value.

Each field in the J-Web configuration editor has the same name as the corresponding configuration statement at the same hierarchy level in the CLI. The options on this page match the options displayed when you enter **edit accounting options** in the CLI:

```
user@router# edit accounting-options ?
Possible completions:
  <[Enter]>      Execute this command
  > class-usage-profile  Class usage profile for accounting data
  > file           Accounting data file configuration
  > filter-profile   Filter profile for accounting data
  > interface-profile Interface profile for accounting data
  > mib-profile     MIB profile for accounting data
  > policy-decision-statistics-profile
                  Profile for policy decision bulkstats
  > routing-engine-profile Routing Engine profile for accounting data
  |              Pipe through a command

[edit]
```


PART 3

Administration

- [Session and User Management on page 45](#)
- [Secure Web Access on page 47](#)
- [Alarms on page 51](#)
- [Events on page 55](#)
- [Device Management on page 63](#)
- [Monitoring in J-Web on page 69](#)
- [Configuration and File Management on page 85](#)

CHAPTER 6

Session and User Management

- [Setting J-Web Session Limits on page 45](#)
- [Terminating J-Web Sessions on page 46](#)
- [Viewing Current Users on page 46](#)

Setting J-Web Session Limits

By default, an unlimited number of users can log in to the J-Web interface on a routing platform, and each session remains open for 24 hours (1440 minutes). Using CLI commands, you can limit the maximum number of simultaneous J-Web user sessions and set a default session timeout for all users.

- To limit the number of simultaneous J-Web user sessions, enter the following commands:

```
user@host# edit system services web-management session
user@host# set session-limit session-limit
```

Range: 1 through 1024. Default: Unlimited

- To change the J-Web session idle time limit, enter the following commands:

```
user@host# edit system services web-management session
user@host# set idle-timeout minutes
```

Range: 1 through 1440. Default: 1440

You can also configure the maximum number of simultaneous subordinate HTTP processes that the routing platform creates in response to user requests.

To configure the maximum number of subordinate httpd processes, enter the following commands:

```
user@host# edit system services web-management limits
user@host# active-child-process process-limit
```

The default is 5, and the range is 0 through 32.

For more information about system services statements, see the [Junos OS System Basics Configuration Guide](#).

Terminating J-Web Sessions

To explicitly terminate a J-Web session at any time, click **Logout** in the top pane. You must log in again to begin a new session.

By default, if the routing platform does not detect any activity through the J-Web interface for 24 hours, the session times out and is terminated. For information about changing the idle time limit, see [“Setting J-Web Session Limits” on page 45](#).

Viewing Current Users

To view a list of users logged in to the routing platform, select **Monitor>System View>System Information** in J-Web and scroll down to the Logged-in User Details section, or enter the **show system users** command in the CLI. The J-Web page and CLI output show all users logged in to the routing platform from either J-Web or the CLI.

CHAPTER 7

Secure Web Access

- [Configuring Secure Web Access on page 47](#)

Configuring Secure Web Access

Navigate to the Management Access Configuration page by selecting **Configure>System Properties>Management Access**. Click **Edit** from the main pane to open the Edit Management Access page. On this page, you can enable HTTP and HTTPS access on interfaces for managing Services Routers through the Web interface. You can also install SSL certificates and enable JUNOScript over SSL with the Secure Access page.

[Figure 13 on page 47](#) shows the Edit Management Access page.

Figure 13: Edit Management Access Page

The figure displays two side-by-side screenshots of the 'Edit Management Access' configuration page in the Juniper J-Web interface.

Left Screenshot (Services Tab):

- Services:** Includes checkboxes for 'Enable telnet' (checked), 'Enable SSH' (checked), 'Enable HTTP' (checked), and 'Enable HTTPS' (unchecked).
- JUNOScript:** Includes checkboxes for 'Enable JUNOScript over clear text' (checked) and 'Enable JUNOScript over SSL' (unchecked). A dropdown menu for 'JUNOScript certificate:' is present.
- HTTP Configuration:** Under 'Enable HTTP', there is a section for 'Enable on all interfaces'. It features a 'Selected interfaces' list and an 'Available interfaces' list containing 'ge-0/0/0.0' and 'lo0.0'.
- HTTPS Configuration:** Under 'Enable HTTPS', there is a section for 'Enable on all interfaces'. It features a 'Selected interfaces' list and an 'Available interfaces' list containing 'ge-0/0/0.0' and 'lo0.0'. A dropdown menu for 'HTTPS certificate:' is also present.
- Buttons:** 'OK' and 'Cancel' buttons are at the bottom.

Right Screenshot (Certificates Tab):

- Certificate names:** A list box for existing certificates, with 'Add...', 'Edit...', and 'Delete' buttons to its right.
- Add certificate:** A section for adding a new certificate, including a 'Certificate name:' text field and a 'Certificate content:' text area.
- Buttons:** 'Save', 'OK', and 'Cancel' buttons are at the bottom.

To configure Web access settings in the J-Web interface:

1. Enter information into the Edit Management Access page, as described in [Table 11 on page 48](#).
2. Click **OK** to apply the configuration.

3. To verify that Web access is enabled correctly, connect to the router using one of the following methods:
 - For HTTP access—In your Web browser, type **http://URL** or **http://IP address**.
 - For HTTPS access—In your Web browser, type **https://URL** or **https://IP address**.
 - For SSL JUNOScript access—A JUNOScript client such as Junos Scope is required. For information about how to log in to Junos Scope, see the *Junos Scope Software User Guide*.

Table 11: Secure Access Configuration Summary

Field	Function	Your Action
Adding Certificates		
Certificate names	<p>Displays digital certificates required for SSL access to the routing platform.</p> <p>Allows you to add and delete SSL certificates.</p> <p>For information about how to generate an SSL certificate, see “Generating SSL Certificates” on page 19.</p>	<p>To add a certificate:</p> <ol style="list-style-type: none"> 1. Click Add on the Certificates tab to display the Add certificate box. 2. Type a name in the Certificate name box—for example, new. 3. Paste the generated certificate and RSA private key in the Certificate content box. <p>To delete a certificate, select it from the list and click Delete.</p>
Enabling HTTP Web Access		
Enable HTTP	Enables HTTP access on interfaces.	To enable HTTP access, select the Enable HTTP access check box on the Services tab.
Enable HTTP on all interfaces	Enables HTTP access on all interfaces at one time.	To enable HTTP access on all interfaces, select the Enable on all interfaces check box on the Services tab.
Selected interfaces	Lists the interfaces for which you want to enable HTTP access.	<p>Clear the Enable on all interfaces check box on the Services tab, select the interface, and move it to the appropriate list by clicking the direction arrows:</p> <ul style="list-style-type: none"> • To enable HTTP access on an interface, move the interface to the Selected interfaces list. • To disable HTTP access on an interface, move the interface to the Available interfaces list.
Enabling HTTPS Web Access		
Enable HTTPS	Enables HTTPS access on interfaces.	To enable HTTPS access, select the Enable HTTPS access check box on the Services tab.
HTTPS certificate	<p>Specifies SSL certificates to be used for encryption.</p> <p>This field is available only after you have created an SSL certificate.</p>	To specify the HTTPS certificate, select a certificate from the HTTPS certificate list on the Services tab—for example, new .

Table 11: Secure Access Configuration Summary (*continued*)

Field	Function	Your Action
Enable on all interfaces	Enables HTTPS on all interfaces at one time.	To enable HTTPS on all interfaces, select the Enable HTTPS on all interfaces check box on the Services tab.
Selected interfaces	Lists interfaces for which you want to enable HTTPS access.	<p>Clear the Enable on all interfaces check box on the Services tab, select the interface, and move it to the appropriate list by clicking the direction arrows:</p> <ul style="list-style-type: none"> To enable HTTPS access on an interface, move the interface to the Selected interfaces list. To disable HTTPS access on an interface, move the interface to the Available interfaces list.
Enabling JUNOScript over SSL		
Enable JUNOScript over SSL	Enables secured SSL access to the JUNOScript XML scripting API.	To enable SSL access, select the Enable JUNOScript over SSL check box on the Services tab.
JUNOScript certificate	<p>Specifies SSL certificates to be used for encryption.</p> <p>This field is available only after you create at least one SSL certificate.</p>	To enable an SSL certificate, select a certificate from the JUNOScript certificate list on the Services tab—for example, new .

CHAPTER 8

Alarms

- [Using Alarms on page 51](#)
- [View Alarms on page 51](#)
- [Active Alarms Information on page 52](#)
- [Alarm Severity on page 52](#)
- [Displaying Alarm Descriptions on page 53](#)
- [Sample Task—Viewing and Filtering Alarms on page 53](#)

Using Alarms

You can monitor active alarms on the J-Web interface. The View Alarms page alerts you about conditions that might prevent the routing platform from operating normally. The page displays information about active alarms, the severity of the alarms, the time at which the alarm began, and a brief description for each active alarm. Alternatively, you can use the CLI to view alarms on all routing platforms. An alarm indicates that you are running the routing platform in a manner that is not recommended. When you see an alarm, you must check its cause and remedy it.

Alternatively, you can display alarm information by entering the following commands at the J-Web CLI terminal:

- **show chassis alarms**
- **show system alarms**

For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the commands, see the *Junos OS System Basics and Services Command Reference*.

View Alarms

On J Series routers only, you can monitor active alarms on the J-Web interface. To view the alarms page, click **Monitor > Events and Alarms > Alarms**. The View Alarms page alerts you about conditions that might prevent the routing platform from operating normally. The page displays information about active alarms, the severity of the alarms, the time at which the alarm began and a brief description for each active alarm. Alternatively, you can use the CLI to view alarms on all routers. An alarm indicates that you are running the

routing platform in a manner that is not recommended. When you see an alarm, you must check its cause and remedy it.

Alternatively, you can display alarm information by entering the following commands at the J-Web CLI terminal:

- **show chassis alarms**
- **show system alarms**

The View Alarms page displays all the active alarms along with detailed descriptions. Each description provides more information about the probable cause or solution for the condition that caused the alarm (see [“Sample Task—Viewing and Filtering Alarms” on page 53](#)). The description also provides the date and time when the failure was detected.

Active Alarms Information

The View Alarms page displays the following types of alarms. You can set the conditions that trigger alarms on an interface. Chassis and system alarm conditions are preset.

- **Interface alarms**—Indicate a problem in the state of the physical links on a fixed or installed Physical Interface Module (PIM), such as a link failure or a missing signal. To enable interface alarms, you must configure them.
- **Chassis alarms**—Indicate a failure on the routing platform or one of its components, such as a power supply failure, excessive component temperature, or media failure. Chassis alarms are preset and cannot be modified.
- **System alarms**—Indicate a missing rescue configuration or software license, where valid. System alarms are preset and cannot be modified.

Alarm Severity

Alarms displayed on the View Alarms page can have the following two severity levels:

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

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

Displaying Alarm Descriptions

All active alarms are displayed on the View Alarms page with detailed description of the alarm. This description provides more information about the probable cause or solution for the condition that caused the alarm (see [“Sample Task—Viewing and Filtering Alarms” on page 53](#)). The description also provides the date and time when the failure was detected. Note the date and time of an alarm so that you can correlate it with error messages on the View Events page or in the messages system log file.

Sample Task—Viewing and Filtering Alarms

Figure 14 on page 53 shows the View Alarms page displaying one system alarm that is currently active. The yellow color indicates that the alarm is noncritical. You can also see the time at which the system received the alarm. You can also filter alarms based on alarm type, severity, description, and date.

Figure 14: View Alarms Page

View Alarms

Alarm filter

Alarm type: Severity:

Description:

Date From: To:

Alarm Details

Type	Severity	Description	Time
System	Minor	Rescue configuration is not set	2008-12-22 08:31:01 UTC

CHAPTER 9

Events

- [Using View Events on page 55](#)
- [Viewing Events on page 56](#)
- [View Events on page 56](#)
- [Understanding Severity Levels on page 57](#)
- [Using Filters on page 57](#)
- [Using Regular Expressions on page 59](#)
- [Sample Task—Filtering and Viewing Events on page 60](#)

Using View Events

The Events task on the J-Web interface enables you to filter and view system log messages that record events occurring on your routing platform.

[Figure 15 on page 56](#) shows the View Events page. This page provides an easy method to view the events recorded in the system log (also known as system log messages). By default, the View Events page displays a summary of the most recent 25 events, with severity levels highlighted in different colors.

The events summary includes information about the time the event occurred, the name of the process that generated the message, the event ID, and a short description of the event. You can move the cursor over the question mark (?) next to an event ID to display a useful description of the event.

You can filter events by system log filename, event ID, text from the event description, name of the process that generated the event, or time period, to display only the events you want. You can also generate and save an HTML report of the system alarms.

Alternatively, enter the following command in the J-Web CLI terminal to display the list of messages and a brief description of each message. For more information about the CLI terminal, see [“Using the CLI Terminal” on page 32](#).

```
user@host> help syslog ?
```

Figure 15: View Events page

View Events

Events Filter

System Log File: Process:

☐ Include archived files

Date From: To:

Event ID: Description:

Events Detail

Process	Severity	Event ID	Event Description	Time
xrtpd			kernel time sync enabled 2001	2009-07-17 04:36:58 PDT
xrtpd			kernel time sync enabled 6001	2009-07-17 04:21:55 PDT
checklogin	notice	WEB_AUTH_SUCC.	Authenticated httpd client (username root)	2009-07-17 04:09:54 PDT

Viewing Events

The View Events page displays system log messages that record events occurring on the routing platform. Events recorded include those of the following types:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process
- Emergency or critical conditions, such as routing platform power-off due to excessive temperature

For more information about system log messages, see the [Junos OS System Log Messages Reference](#).

View Events

To view system log messages that record events occurring on your routing platform, click **Monitor>Events and Alarms>View Events**. The View Events page is displayed. This page provides an easy method to view the events recorded in the system log (also known as system log messages). By default, the View Events page displays a summary of the most recent 25 events, with severity levels highlighted in different colors.

The View Events page displays system log messages that record events occurring on the routing platform. Events recorded include those of the following types:

- Routine operations, such as creation of an OSPF protocol adjacency or a user login into the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a child or peer process

- Emergency or critical conditions, such as routing platform power-off due to excessive temperature

On the View Events page, you can also use filters to display relevant events. [Table 13 on page 58](#) lists the different filters, their functions, and the associated actions. You can apply any or a combination of the described filters to view the messages that you want to view. After specifying the filter or filters you want, click **Search** to display the filtered events.

Understanding Severity Levels

On the View Events page, the severity level of a message is indicated by different colors. The severity level indicates how seriously the triggering event affects routing platform functions.

[Table 12 on page 57](#) lists the system log severity levels, the corresponding colors, and a description of what the severity level indicates.

Table 12: Severity Levels

Color	Severity Level (from Highest to Lowest Severity)	Description
Red	emergency	System panic or other conditions that cause the routing platform to stop functioning.
Orange	alert	Conditions that must be corrected immediately, such as a corrupted system database.
Pink	critical	Critical conditions, such as hard drive errors.
Blue	error	Standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
Yellow	warning	Conditions that warrant monitoring.
Green	notice	Conditions that are not error conditions but are of interest or might warrant special handling.
	info	Informational messages. This is the default.
	debug	Software debugging messages.
Gray	unknown	No severity level is specified.

Using Filters

On the View Events page, you can use filters to display relevant events. [Table 13 on page 58](#) lists the different filters, their functions, and the associated actions. You can apply any or a combination of the described filters to view the messages that you want

to view. After specifying the filter or filters you want, click **Search** to display the filtered events. Click **Reset** to clear the existing search criteria and enter new values.

Table 13: Summary of Event Filters

Event Filter	Function	Your Action
System Log File	<p>Specifies the name of a system log file for which you want to display the recorded events.</p> <p>The list includes the names of all the system log files that you configure.</p> <p>By default, a log file, messages, is included in the /var/log/ directory.</p> <p>For information about how to configure system log files, see the Junos OS System Log Messages Reference.</p>	To specify events recorded in a particular file, select the system log filename from the list—for example, messages .
Event ID	<p>Specifies the event ID for which you want to display the messages.</p> <p>If you type part of the ID, the system completes the remaining ID automatically.</p> <p>An event ID, also known as a system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.</p>	To specify events with a specific ID, type its partial or complete ID—for example, TFTPD_AF_ERR .
Description	<p>Specifies text from the description of events that you want to display.</p> <p>You can use a regular expression to match text from the event description.</p> <p>NOTE: The regular expression matching is case-sensitive.</p> <p>For more information about using regular expressions, see “Using Regular Expressions” on page 59.</p>	<p>To specify events with a specific description, type a text string from the description. You can include a regular expression.</p> <p>For example, type ^Initial* to display all messages with lines beginning with the term <i>Initial</i>.</p>
Process	<p>Specifies the name of the process generating the events you want to display.</p> <p>To view all the processes running on your system, enter the CLI command show system processes in the J-Web CLI terminal.</p> <p>For more information about processes, see the Junos OS Installation and Upgrade Guide.</p>	<p>To specify events generated by a process, type the name of the process.</p> <p>For example, type mgd to list all messages generated by the management process.</p>
Include archived files	Includes the archived log files in the search. Files are archived when the active log file reaches its maximum size limit.	Select the check box to include archived files in the search.

Table 13: Summary of Event Filters (*continued*)

Event Filter	Function	Your Action
Date From	Specifies the time period in which the events you want displayed are generated.	To specify the time period:
To	<p>A calendar allows you to select the year, month, day, and time. It also allows you to select the local time.</p> <p>By default, the messages generated in the last one hour are displayed. To shows the current date and time, and Date From shows the time one hour before end time.</p>	<ul style="list-style-type: none"> Click the button next to Date From and select the year, month, date, and time—for example, 02/10/2006 11:32. Click the button next to To and select the year, month, date, and time—for example, 02/10/2006 3:32. <p>To select the current time as the start time, select Local Time.</p>

Using Regular Expressions

On the View Events page, you can filter the events displayed by the text in the event description. In the **Description** box, you can use regular expressions to filter and display a set of messages for viewing. Junos OS supports POSIX Standard 1003.2 for extended (modern) UNIX regular expressions.

Table 14 on page 59 specifies some of the commonly used regular expression operators and the terms matched by them. A term can match either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.



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

Table 14: Common Regular Expression Operators and the Terms They Match

Regular Expression Operator	Matching Terms
. (period)	<p>One instance of any character except the space.</p> <p>For example, .in matches messages with <i>win</i> or <i>windows</i>.</p>
* (asterisk)	<p>Zero or more instances of the immediately preceding term.</p> <p>For example, tre* matches messages with <i>tree</i>, <i>tread</i>, or <i>trough</i>.</p>
+ (plus sign)	<p>One or more instances of the immediately preceding term.</p> <p>For example, tre+ matches messages with <i>tree</i> or <i>tread</i> but not <i>trough</i>.</p>
? (question mark)	<p>Zero or one instance of the immediately preceding term.</p> <p>For example, colou?r matches messages with <i>or color</i> or <i>colour</i>.</p>
(pipe)	<p>One of the terms that appear on either side of the pipe operator.</p> <p>For example, gre ay matches messages with either <i>grey</i> or <i>gray</i>.</p>

Table 14: Common Regular Expression Operators and the Terms They Match (*continued*)

Regular Expression Operator	Matching Terms
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is specific to Junos OS.
^ (caret)	The start of a line, when the caret appears outside square brackets. For example, <code>^T</code> matches messages with <i>This line</i> and not with <i>On this line</i> .
\$ (dollar sign)	Strings at the end of a line. For example, <code>:\$</code> matches messages with <i>the following:</i> and not with <i>2:00</i> .
[] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, <code>[0-9]</code> matches messages with any number.
() (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression. For example, <code>dev(/ ice)</code> matches messages with <i>dev/</i> or <i>device</i> .

Sample Task—Filtering and Viewing Events

Figure 16 on page 61 shows the View Events page displaying filtered events. In this example, you are typing **UI_CHILD_EXITED** in the Event ID box and clicking **Search**. The Event Summary displays messages with the **UI_CHILD_EXITED** event ID only. You can view the following information about the events:

- Messages displayed are green. The green color and context-sensitive help indicate that the message severity level is **notice** and the event type is **error**. This information means that the condition causing the message is an error or failure and might require corrective action.
- The events were generated by the management process (mgd).
- The Event Description column displays a brief description of the event, and the help description provides information about the cause of the event.

Figure 16: J-Web View Events Page

View Events

Events Filter

System Log File: Process:

☐ Include archived files

Date From: To:

Event ID: Description:

Events Detail

Process	Severity	Event ID	Event Description	Time
checklogin	notice	WEB_AUTH_SUC	Authenticated httpd client (username root)	2009-07-17 04:09:54 PDT

CHAPTER 10

Device Management

- [Using Software \(J Series Routing Platforms Only\) on page 63](#)
- [Using Licenses \(J Series Routing Platform Only\) on page 64](#)
- [Using Snapshot \(J Series Routing Platforms Only\) on page 65](#)
- [Sample Task—Manage Snapshots on page 66](#)
- [Using Reboot on page 67](#)

Using Software (J Series Routing Platforms Only)

On J Series routers only, you can upgrade and manage Junos OS packages from the J-Web interface. A Junos OS package is a collection of files that make up the software components of the routing platform.

Typically, you upgrade the Junos OS on a routing platform by downloading a set of images onto your routing platform or onto another system on your local network, such as a PC. You then uncompress the package and install the uncompressed software using the `Maintain>Software` page. Finally, you boot your system with this upgraded device.

As new features and software fixes become available, you must upgrade your software to use them. Before an upgrade, we recommend that you back up your primary boot device in case it becomes corrupted or fails during the upgrade. Creating a backup also stores your active configuration files and log files and ensures that you recover to a known, stable environment in case of an unsuccessful upgrade. For more information about creating a system backup, see [“Sample Task—Manage Snapshots” on page 66](#).

During a successful upgrade, the upgrade package completely reinstalls the existing software. The upgrade process rebuilds the file system but retains configuration files, log files, and similar information from the previous version.

For more information, see the *Junos OS System Basics Configuration Guide*.

[Table 15 on page 64](#) lists the different tasks that you can perform from the `Maintain>Software` pages.

Table 15: Manage Software Tasks Summary

Manage Software Task	Function
Upload Package	<p>Install software packages uploaded from your computer to the routing platform.</p> <ul style="list-style-type: none"> 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 check box is selected, the router is automatically rebooted when the upgrade is complete. Select the check box if you want the router to reboot automatically when the upgrade is complete. <p>Click Upload Package to begin, and click Cancel to clear the entries and return to the previous page.</p>
Install Package	<p>Install software packages on the routing platform that are retrieved with FTP or HTTP from the location specified.</p> <ul style="list-style-type: none"> Package Location—Specifies the FTP or HTTP server, file path, and software package name. The software is activated after the router has rebooted. User—Specifies the username, if the server requires one. Password—Specifies the password, if the server requires one. Reboot If Required—If this check box is selected, the router is automatically rebooted when the upgrade is complete. <p>Click Fetch and Install Package to begin.</p>
Downgrade	<p>Downgrade the Junos OS on the routing platform.</p> <p>When you downgrade the software to a previous version, the software version that is saved in junos.old is the version of Junos OS that your router is downgraded to. For your changes to take effect, you must reboot the router.</p> <p>CAUTION: After you perform this operation, you cannot undo it.</p>

Alternatively, you can install software packages on your routing platform by entering the **request system software add** command at the J-Web CLI terminal.

Using Licenses (J Series Routing Platform Only)

The Maintain>Licenses page displays a summary of the licenses needed and used for each feature that requires a license on a J Series routing platform. This page also allows you to add licenses.

To enable some Junos OS features on a J Series routing platform, you must purchase, install, and manage separate software licenses. The presence on the router of the appropriate software license keys (passwords) determines the features you can configure and use. Each feature license is tied to exactly one software feature, and that license is valid for exactly one J Series routing platform.

Using the Maintain>Licenses page, you can perform the following tasks:

- Add licenses—Add license keys for the following features:
 - Data link switching (DLSw) support

- Flow monitoring traffic analysis support
- Advanced Border Gateway Protocol (BGP) features that enable route reflectors for readvertising BGP routes to internal peers.
- Delete licenses—Delete one or more license keys from a J Series routing platform with the J-Web license manager.
- Display license keys—Display the license keys in text format. Multiple licenses are separated by a blank line.

Alternatively, you can run the following commands at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the commands, see the *Junos OS System Basics and Services Command Reference*.

- **show system license**—Display license information.
- **request system license add**—Add licenses on J Series routers.

For more information about licenses, see the Getting Started Guide for your J Series router.

Using Snapshot (J Series Routing Platforms Only)

The Maintain>Snapshot page allows you to configure storage devices to replace the primary boot device on your router or to act as a backup boot device. To do so, you create a snapshot of the system software running on your router, saving the snapshot to an alternative storage device.

The Manage Snapshot page allows you to perform the following tasks:

- Copy the current system software, along with the current and rescue configurations, to an alternative storage device.



CAUTION: We recommend that you keep your secondary storage medium updated at all times. If the internal compact flash fails at startup, the J Series routing platform automatically boots itself from this secondary storage medium. The secondary storage medium can be either an external compact flash or a USB storage device. When a secondary storage medium is not available, the routing platform is unable to boot and does not come back online. This situation can occur if the power fails during a Junos OS upgrade and the physical or logical storage media on the routing platform are corrupted. The backup device must have a storage capacity of at least 256 MB.

- Copy only default files that were loaded on the internal compact flash when it was shipped from the factory, plus the rescue configuration, if one has been set.
- Configure a boot device to store snapshots of software failures, for use in troubleshooting.

- Partition the storage medium. This process is usually necessary for storage devices that do not already have software installed on them.
- Create a snapshot for use as the primary boot device to replace the device in the internal compact flash slot or to replicate it for use in another J Series routing platform. You can perform this action only on a removable storage device.
- Specify the size of the following partitions in kilobytes:
 - **data**—Data partition is not used by the routing platform, and can be used for extra storage.
 - **swap**—Swap partition is used for swap files and software failure memory snapshots. Software failure memory snapshots are saved to the boot medium only if it is specified as the dump device.
 - **config**—Config partition is used for storing configuration files.
 - **root**—Root partition does not include configuration files.

Click **Snapshot** to begin.

Alternatively, you can use the **request system snapshot** command in the J-Web CLI terminal to take a snapshot of the routing platform. For information about installing boot devices, see the Getting Started Guide for your J Series router.

Sample Task—Manage Snapshots

Figure 17 on page 67 shows a Maintain>Snapshot page that allows you to back up the currently running and active file system on a standby storage device that is not running. In this example, you are taking the snapshot to replace the current primary boot device on the routing platform. A compact flash is connected to the USB port on the J Series routing platform with a USB adapter.

To take the snapshot:

1. Select **Maintain>Snapshot** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 17 on page 67).
3. Select **compact-flash** from the Target Media list to specify the storage device to copy the snapshot to.
4. Next to As Primary Media, select the check box to create a storage medium to be used in the internal compact flash slot only.
5. Click **Snapshot**.

Figure 17: Manage Snapshots Page

Snapshot

System Snapshot

You can configure boot devices to replace the primary boot device or to act as a backup boot device. To do this, you create a snapshot of the running system software, saving the snapshot to an alternate media.

The snapshot process copies the current system software, along with the current and rescue configurations, to alternate media. Optionally, you can copy only the factory and rescue configurations.

Target Media: Snapshots the system software to specified media:

- compact-flash: Internal compact flash
- removable-compact-flash: External compact flash

Target Media

compact-flash

?

Factory

☐

?

Partition

☐

?

Advanced options

As Primary Media

☒

?

Data Size

?

Swap Size

?

Config Size

?

Root Size

?

Snapshot

Using Reboot

The Maintain>Reboot page allows you to reboot the routing platform at a specified time. Using the Maintain>Reboot page, you can perform the following tasks:

- Reboot the router immediately, after a specified number of minutes or at the absolute time that you specify, on the current day.
- Stop (halt) the router software immediately. After the router software has stopped, you can access the router through the console port only.
- Type a message to be displayed to any users on the router before the reboot occurs.

Click **Schedule** to begin.

If the reboot is scheduled to occur immediately, the router reboots. You cannot access the J-Web interface until the router has restarted and the boot sequence is complete. After the reboot is complete, refresh the browser window to display the J-Web interface login page.

Alternatively, you can reboot the routing platform by running the **request system reboot** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the **request system reboot** command, see the [Junos OS System Basics and Services Command Reference](#).

CHAPTER 11

Monitoring in J-Web

- [Monitor Task Overview on page 69](#)
- [Chassis Viewer \(M7i, M10i, M20, M120, and M320 Routing Platforms Only\) on page 70](#)
- [Class of Service on page 71](#)
- [Interfaces on page 72](#)
- [MPLS on page 73](#)
- [PPPoE \(J Series Routing Platforms Only\) on page 74](#)
- [RPM on page 74](#)
- [Routing on page 75](#)
- [Security on page 76](#)
- [Service Sets on page 78](#)
- [Services on page 78](#)
- [System View on page 79](#)
- [Sample Task—Monitoring Interfaces on page 81](#)
- [Sample Task—Monitoring Route Information on page 82](#)

Monitor Task Overview

Use the J-Web Monitor tasks to monitor your routing platform. The J-Web interface displays diagnostic information about the routing platform in the browser.

You can also monitor the routing platform with command-line interface (CLI) operational mode commands that you type into a CLI emulator in the J-Web interface. The monitoring pages display the same information displayed in the output of **show** commands entered in the CLI terminal. For more information about the J-Web CLI terminal, see [“Using the CLI Terminal” on page 32](#). For more information about the **show** commands, see the Junos OS command references.

J-Web monitoring pages appear when you select **Monitor** in the taskbar. The monitoring pages display the current configuration on your system and the status of your system, chassis, interfaces, and routing and security operations. The monitoring pages have plus signs (+) that you can expand to view details. On some pages, such as the Routing Information page, you can specify search criteria to view selective information.

Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only)

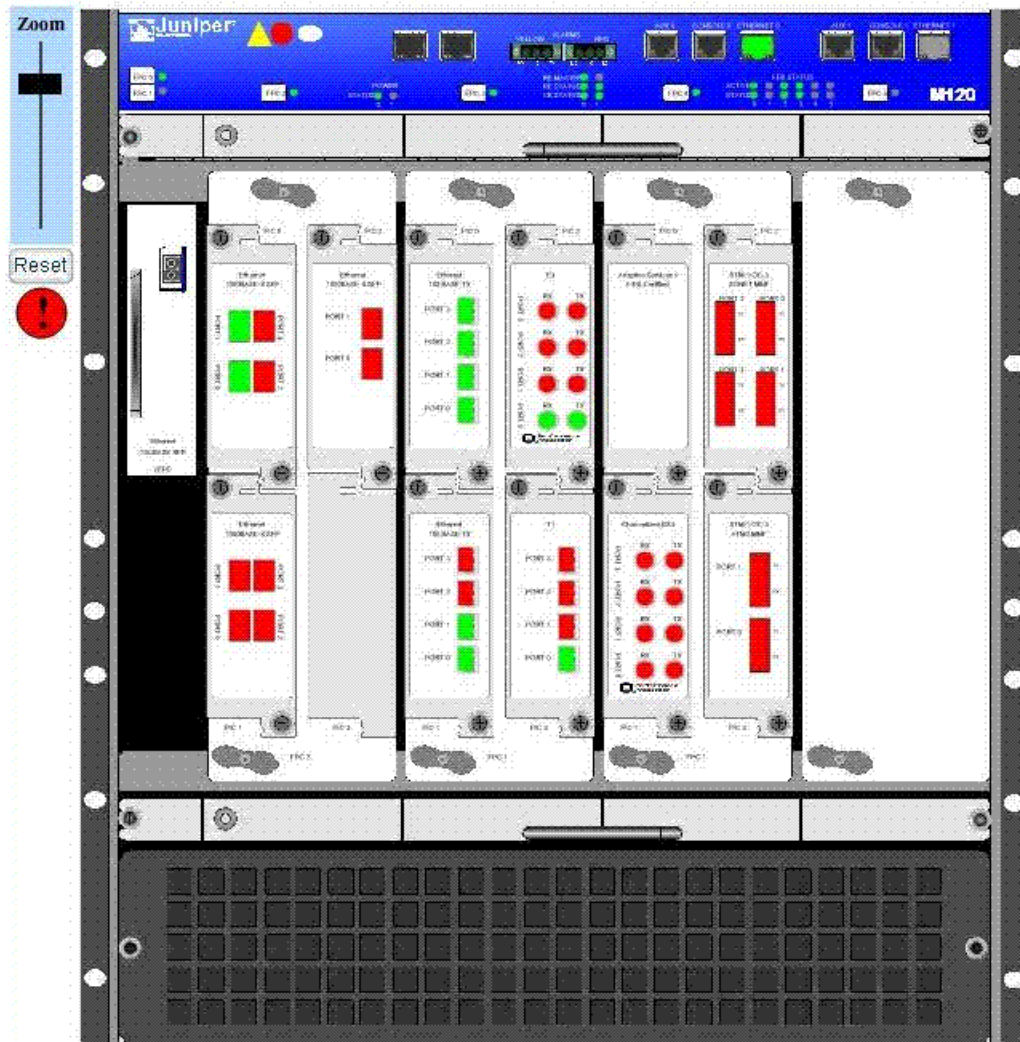
On M7i, M10i, M20, M120, and M320 routers, you can use the chassis viewer feature to view images of the chassis and access information about each component similar to what you can obtain using the **show chassis alarms** and **show chassis hardware** commands.

To access the chassis viewer, click **Chassis** in the upper-right corner of any J-Web page for an M7i, M10i, M20, M120, or M320 routing platform. A separate page appears to display the image of the chassis and its component parts, including power supplies, individual Physical Interface Cards (PICs), and ports. Major or minor alarm indicators appear in red.

[Figure 18 on page 71](#) shows the chassis and components of an M120 routing platform. It also shows the status of each port in red or green, and the zoom bar selections.

Figure 18: Chassis Viewer Page

Click and drag the chassis to pan the image. Hover over a FRU for status information (serial number, description, etc.). Right click on the chassis for more options such as configuration and monitoring. Router status lights are updated every 1 minute.



Class of Service

To display details about the performance of class of service (CoS) on a routing platform, select **Monitor > Class of Service** in the J-Web interface.

Table 16 on page 72 shows a summary of the information displayed on the Class of Service pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

Table 16: Class of Service Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Interfaces	
Information about the physical and logical interfaces in the system and details about the CoS components assigned to these interfaces.	show class-of-service interface
Classifiers	
Forwarding classes and loss priorities that incoming packets are assigned to based on the packet's CoS values.	show class-of-service classifier
CoS Value Aliases	
CoS value aliases that the system is using to represent DiffServ code point (DSCP), DSCP IPv6, MPLS experimental (EXP), and IPv4 precedence bits.	show class-of-service code-point-aliases
RED Drop Profiles	
Detailed information about the drop profiles used by the system. Also, displays a graph of the random early detection (RED) curve that the system uses to determine the queue fullness and drop probability.	show class-of-service drop-profile
Forwarding Classes	
Assignment of forwarding classes to queue numbers.	show class-of-service forwarding-class
Rewrite Rules	
Packet CoS value rewrite rules based on the forwarding classes and loss priorities.	show class-of-service rewrite-rule
Scheduler Maps	
Assignment of forwarding classes to schedulers. Schedulers include transmit rate, rate limit, and buffer size.	show class-of-service scheduler-map

Interfaces

The J-Web interface hierarchically displays all routing platform physical and logical interfaces, including state and configuration information. This information is divided into multiple parts. To view general interface information such as available interfaces, operation states of the interfaces, and descriptions of the configured interfaces, select **Monitor>Interfaces** in the J-Web interface. To view interface-specific properties such as administrative state or traffic statistics in the J-Web interface, select the interface name on the Port Monitoring page and click **Details**. (See [“Sample Task—Monitoring Interfaces”](#) on page 81.)

[Table 17 on page 73](#) shows a summary of the information displayed on the Interfaces pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 17: Interfaces Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Status information about the specified Protocol Independent Multicast (PIM).	show interfaces terse
Detailed information about all interfaces configured on the routing platform.	show interfaces detail
Current state of the interface you specify.	show interfaces <i>interface-name</i>

MPLS

To view information about MPLS label-switched paths (LSPs) and virtual private networks (VPNs), select **Monitor>MPLS**.

[Table 18 on page 73](#) shows a summary of the information displayed on the MPLS pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

Table 18: MPLS Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Interfaces	
Interfaces on which MPLS is enabled, plus the operational state and any administrative groups applied to an interface.	show mpls interface
LSP Information	
LSP sessions currently active on the routing platform, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	show mpls lsp
LSP Statistics	
Statistics for LSP sessions currently active on the routing platform, including the total number of packets and bytes forwarded through an LSP.	show mpls lsp statistics
RSVP Sessions	
RSVP-signaled LSP sessions currently active on the routing platform, including inbound (ingress) and outbound (egress) addresses, LSP state, and LSP name.	show rsvp session
RSVP Interfaces	
Interfaces on which RSVP is enabled, including the interface name, total bandwidth through the interface, and total current reserved and reservable (available) bandwidth on the interface.	show rsvp interface

PPPoE (J Series Routing Platforms Only)

The Point-to-Point Protocol over Ethernet (PPPoE) monitoring information is displayed in multiple parts. To display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the routing platform, and the PPPoE version configured on the routing platform, select **Monitor>PPPoE** in the J-Web interface.

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

[Table 19 on page 74](#) shows a summary of the information displayed on the PPPoE page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 19: PPPoE Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Session-specific information about the interfaces on which PPPoE is enabled.	show pppoe interfaces
Statistics for PPPoE sessions currently active.	show pppoe statistics
PPPoE protocol currently configured on the routing platform.	show pppoe version

RPM

The real-time performance monitoring (RPM) information includes the round-trip time, jitter, and standard deviation values for each configured RPM test on the routing platform. To view these RPM properties, select **Troubleshoot > RPM** in the J-Web interface.

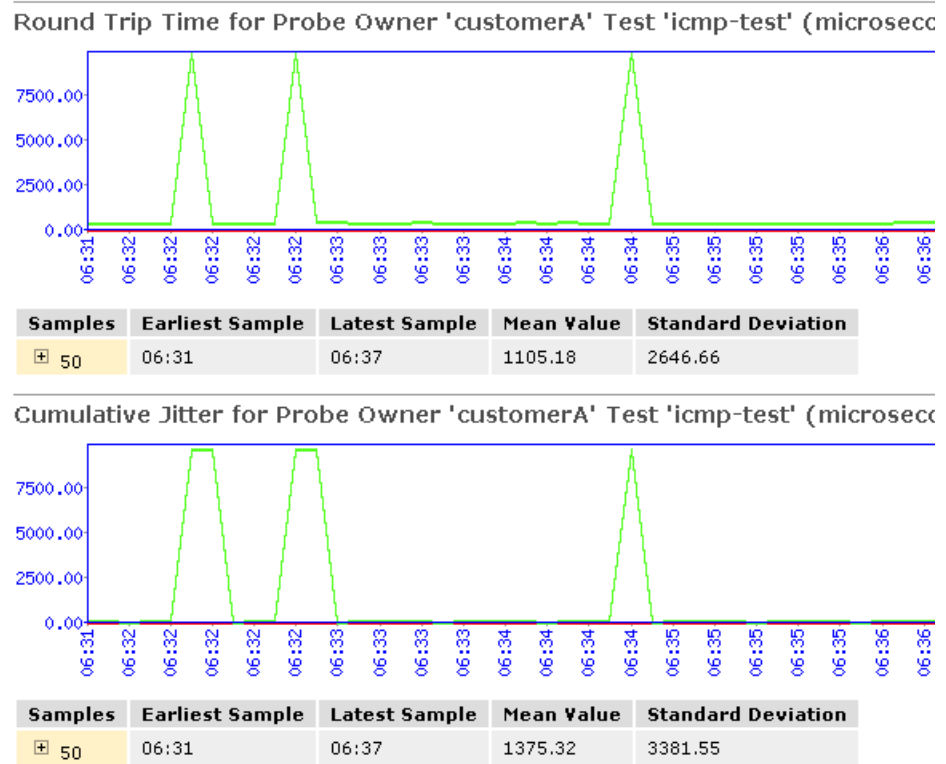
[Table 20 on page 74](#) shows a summary of the information displayed on the RPM page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

Table 20: RPM Information and the Corresponding CLI show Command

Information Displayed	Corresponding CLI Command
Results of the most recent RPM probes.	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 19 on page 75](#) shows sample graphs for an RPM test.

Figure 19: Sample RPM Graphs



In [Figure 19 on page 75](#), the round-trip time and jitter values are plotted as a function of the system time. Large spikes in round-trip time or jitter indicate a slower outbound (egress) or inbound (ingress) time for the probe sent at that particular time.

Routing

To view information about routes in a routing table or for information about OSPF, BGP, RIP, or data link switching (DLSw), select **Monitor>Routing** in the J-Web interface.

The routing information includes information about the route's destination, protocol, state, and parameters. To view selective information, type or select information in one or more of the Narrow Search boxes, and click **Search**.

[Table 21 on page 75](#) shows a summary of the information displayed on the Routing pages and the corresponding CLI **show** commands that you can enter at the J-Web CLI terminal.

Table 21: Routing Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Route Information	
A high-level summary of the routes in the routing table.	show route terse
Detailed information about the active entries in the routing tables.	show route detail

Table 21: Routing Information and the Corresponding CLI show Commands (*continued*)

Information Displayed	Corresponding CLI Command
BGP Information	
Summary about Border Gateway Protocol (BGP).	show bgp summary
BGP peers.	show bgp neighbor
OSPF Information	
Information about OSPF neighbors.	show ospf neighbors
OSPF interfaces.	show ospf interfaces
OSPF statistics.	show ospf statistics
RIP Information	
Routing Information Protocol (RIP) statistics about messages sent and received on an interface, as well as information received from advertisements from other routers.	show rip statistics
RIP neighbors.	show rip neighbors
DLSw Information	
Data link switching (DLSw) capabilities of a specific remote peer or all peers.	show dlsw capabilities
Configured DLSw circuits.	show dlsw circuits
DLSw peer status.	show dlsw peers
Media access control (MAC) and IP addresses of remote DLSw peers.	show dlsw reachability

Security

- [Firewall on page 76](#)
- [IPsec on page 77](#)
- [NAT on page 77](#)

Firewall

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

Table 22 on page 77 shows a summary of the information displayed on Firewall pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 22: Firewall Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Statistics Summary	
Stateful firewall filter statistics.	show services stateful-firewall statistics
Stateful Firewall	
Stateful firewall filter conversations.	show services stateful-firewall conversations
Flow table entries for stateful firewall filters.	show services stateful-firewall flows
IDS Information	
Information about an address under possible attack.	show services ids destination-table
Information about an address that is a suspected attacker.	show services ids source-table
Information about a particular suspected attack source-and-destination address pair.	show services ids pair-table

IPsec

To view information about configured IP Security (IPsec) tunnels and statistics, and Internet Key Exchange (IKE) security associations for adaptive services interfaces, select **Monitor>Security>IPsec** in the J-Web interface.

Table 23 on page 77 shows a summary of the information displayed on the IPsec page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 23: IPsec Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
(Adaptive services interface only) IPsec statistics for the selected service set.	show services ipsec-vpn ipsec statistics
(Adaptive services interface only) IPsec security associations for the selected service set.	show services ipsec-vpn ipsec security-associations
(Adaptive services interface only) Internet Key Exchange (IKE) security associations.	show services ipsec-vpn ike security-associations

NAT

NAT pool information includes information about the address ranges configured within the pool on the routing platform. To view NAT pool information, select **Monitor>Security>NAT** in the J-Web interface.

Table 24 on page 78 shows a summary of the information displayed on the NAT page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

Table 24: NAT Information and the Corresponding CLI show Command

Information Displayed	Corresponding CLI Command
Information about Network Address Translation (NAT) pools.	show services nat pool

Service Sets

Service set information includes the services interfaces on the routing platform, the number of services sets configured on the interfaces, and the total CPU used by the service sets. To view these service set properties, select **Monitor>Service Sets** in the J-Web interface.

A service set is a group of rules from a stateful firewall filter, Network Address Translation (NAT), intrusion detection service (IDS), or IP Security (IPsec) that you apply to a services interface. IDS, NAT, and stateful firewall filter service rules can be configured within the same service set. However, IPsec services are configured in a separate service set.

Table 25 on page 78 shows a summary of the information displayed on Service Sets pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 25: Service Sets Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Service set summary information.	show services service-sets summary
Service set memory usage.	show services service-sets memory-usage

Services

A J Series routing platform can operate as a Dynamic Host Configuration Protocol (DHCP) server. To view information about dynamic and static DHCP leases, conflicts, pools, and statistics, select **Monitor>Services>DHCP** in the J-Web interface.

Table 26 on page 78 shows a summary of the information displayed on the DHCP page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 26: DHCP Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
DHCP server client binding information.	show system services dhcp binding
DHCP client-detected conflicts for IP addresses.	show system services dhcp conflict
DHCP server IP address pools.	show system services dhcp pool

Table 26: DHCP Information and the Corresponding CLI show Commands (*continued*)

Information Displayed	Corresponding CLI Command
DHCP server statistics.	show system services dhcp statistics

System View

- [System Information on page 79](#)
- [Chassis Information on page 79](#)
- [Process Details on page 80](#)
- [FEB Redundancy \(M120 Routing Platforms Only\) on page 80](#)

System Information

To view information about system properties such as the name and IP address of the routing platform or the resource usage on the Routing Engine, select **Monitor>System View** in the J-Web interface.

[Table 27 on page 79](#) shows a summary of the information displayed on System pages and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 27: System Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Current time and information about how long the routing platform, routing platform software, and routing protocols have been running.	show system uptime
Information about users who are currently logged in to the routing platform.	show system users
Statistics about the amount of free disk space in the routing platform's file systems.	show system storage
Software processes running on the routing platform.	show system processes

Chassis Information

To view chassis properties on the routing platform, select **Monitor>System View>Chassis Information** in the J-Web interface.

[Table 28 on page 80](#) shows a summary of the information displayed on the Chassis Information page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 28: Chassis Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Conditions that have been configured to trigger alarms.	show chassis alarms
Environmental information about the routing platform chassis, including the temperature and information about the fans, power supplies, and Routing Engine.	show chassis environment
Status information about the installed FPCs and PICs.	show chassis fpc
List of all FPCs and PICs installed in the routing platform chassis, including the hardware version level and serial number.	show chassis hardware

Process Details

To view process details like process ID, CPU load, or memory utilization, select **Monitor>System View>Process Details** in the J-Web interface.

[Table 29 on page 80](#) shows a summary of the information displayed on the Process Details page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 29: Process Details Information and the Corresponding CLI show Commands

Information Displayed	Corresponding CLI Command
Software processes running on the router	show processes extensive

FEB Redundancy (M120 Routing Platforms Only)

On M120 routers, Forwarding Engine Boards (FEBs) provide route lookup and forwarding functions from Flexible PIC Concentrators (FPCs) and compact Flexible PIC Concentrators (cFPCs). You can configure FEB redundancy groups to provide high availability for FEBs.

To view the status of FEBs and FEB redundancy groups, or connectivity between FPCs and FEBs, select **Monitor>System View>FEB Redundancy** in the J-Web interface.

[Table 30 on page 80](#) shows a summary of the information displayed on the FEB Redundancy page and the corresponding CLI **show** command you can enter at the J-Web CLI terminal.

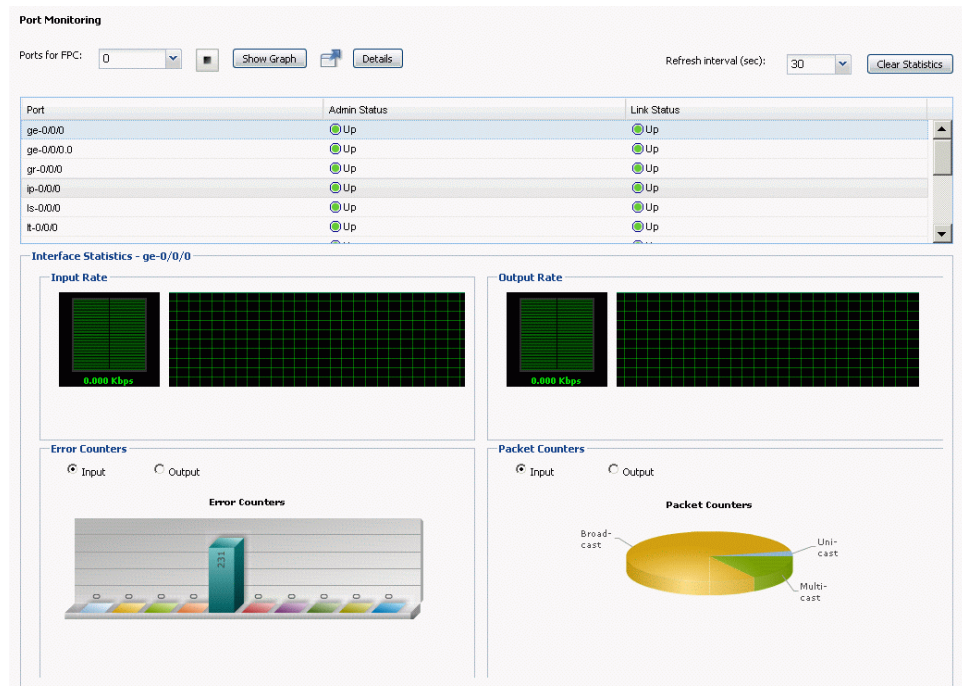
Table 30: FEB Redundancy Information and the Corresponding CLI show Command

Information Displayed	Corresponding CLI Command
Forwarding Engine Board (FEB) status information.	show chassis feb

Sample Task—Monitoring Interfaces

Figure 20 on page 81 shows the Port Monitoring page that displays the interfaces installed on your routing platform. At a glance, you can monitor the status of all the configured physical and logical interfaces.

Figure 20: Port Monitoring Page



You can select any interface and click **Details** to view details about its status. For example, selecting **ge-0/0/0** and clicking **Details**, displays detailed information about the interface (see Figure 21 on page 82).

Figure 21: Details of Interface ge-0/0/0 Page

Name	Value
name	ge-0/0/0
local-index	129
snmp-index	160
generation	132
link type	Ethernet
mtu	1514
source-filtering	disabled
link-mode	Full-duplex
speed	1000mbps
BPDU error	none
MAC-REWRITE Error	none
loopback	disabled
flow control	enabled
auto-negotiation	enabled
remote fault	online
device flags	present running
config flags	snmp-traps flags
media flags	none

OK

Sample Task—Monitoring Route Information

Figure 22 on page 83 shows the Route Information monitoring page that displays information about all 9 routes in the routing table. All routing platforms are active, and there are no hidden routes.

Figure 22: Monitoring Route Information Page with Complete Information

Routing

Route Information

9 destinations, 9 routes (8 active, 0 hold down, 1 hidden) Showing 8 of 9 routes

inet.0

Destination	Protocol/Preference	Next-Hop	Age
+ 0.0.0.0/0	*Static/5	Router	2w2d 19:46:24
+ 10.10.0.0/16	*Static/5	Router	2w2d 19:46:24
+ 10.209.0.0/18	*Direct/0	Interface	2w2d 19:46:24
+ 10.209.8.129/32	*Local/0	Local	2w2d 19:46:26
+ 172.16.0.0/12	*Static/5	Router	2w2d 19:46:24
+ 192.168.0.0/16	*Static/5	Router	2w2d 19:46:24
+ 192.168.102.0/23	*Static/5	Router	2w2d 19:46:24
+ 207.17.136.0/24	*Static/5	Router	2w2d 19:46:24

Narrow Search

Destination Address Protocol

Next Hop Address Receive Protocol

Best Route ☐ Inactive Routes ☐

Exact Route ☐ Hidden Routes ☐

Number of Routes to Display

By default, information about all routes in the routing table (up to a maximum of 25 routes on one page) is displayed. To view information about selective routes, type or select information in one or more of the Narrow Search boxes, and click **OK**. For example, typing **direct** in the box next to Protocol, displays the only 1 route. This is the only route that has **0** preference from a directly connected network. (see [Figure 23 on page 83](#)).

Figure 23: Monitoring Route Information Page with Selective Information

Routing

Route Information

9 destinations, 9 routes (8 active, 0 hold down, 1 hidden) Showing 1 of 9 routes

inet.0

Destination	Protocol/Preference	Next-Hop	Age
+ 10.209.0.0/18	*Direct/0	Interface	2w2d 22:01:22

Narrow Search

Destination Address Protocol

Next Hop Address Receive Protocol

Best Route ☐ Inactive Routes ☐

Exact Route ☐ Hidden Routes ☐

Number of Routes to Display

Configuration and File Management

- [Displaying Configuration History on page 85](#)
- [Displaying Users Editing the Configuration on page 87](#)
- [Loading a Previous Configuration File on page 88](#)
- [Downloading a Configuration File on page 89](#)
- [Comparing Configuration Files on page 89](#)
- [Upload Configuration File on page 90](#)
- [Using Rescue \(J Series Routing Platforms Only\) on page 91](#)
- [Using Files on page 92](#)

Displaying Configuration History

When you commit a configuration, the routing platform saves the current operational version and the previous 49 versions of committed configurations. To manage these configuration files with the J-Web interface, select **Maintain>Config Management>History**. The main pane displays Database Information and Configuration History (see [Figure 24 on page 86](#)).

[Table 31 on page 86](#) summarizes the contents of the display.

The configuration history display allows you to perform the following operations:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the routing platform.

Figure 24: Configuration Database and History Page

History							
Database Information							
No users are editing the configuration database.							
Configuration History							
The following table shows the device's commit history.							
To view a configuration, click the revision number.							
To compare configurations, select two and click "Compare".							
<input type="button" value="Compare"/>							
	Number	Date/Time	User	Client	Comment	Log Message	Action
<input type="checkbox"/>	Current	2008-12-23 09:28:24 UTC	regress	cli			Download
<input type="checkbox"/>	1	2008-12-23 08:16:34 UTC	root	junoscript		Rolled back via Web Interface	Download Rollback
<input type="checkbox"/>	2	2008-12-22 08:33:12 UTC	root	cli			Download Rollback
<input type="checkbox"/>	3	2008-12-22 08:30:49 UTC	root	other			Download Rollback
<input type="checkbox"/>	4	2008-09-30 07:04:28 UTC	root	cli			Download Rollback
<input type="checkbox"/>	5	2008-09-30 06:46:52 UTC	root	cli			Download Rollback
<input type="checkbox"/>	6	2008-09-30 06:44:48 UTC	root	cli			Download Rollback
<input type="checkbox"/>	7	2008-09-30 06:40:08 UTC	root	cli			Download Rollback
<input type="checkbox"/>	8	2008-03-19 19:31:53 UTC	root	cli			Download Rollback

Table 31: J-Web Configuration History Summary

Field	Description
Number	Version of the configuration file.
Date/Time	Date and time the configuration was committed.
User	Name of the user who committed the configuration.

Table 31: J-Web Configuration History Summary (*continued*)

Field	Description
Client	<p>Method by which the configuration was committed:</p> <ul style="list-style-type: none"> • cli—A user entered a Junos OS CLI command. • junoscript—A JUNOScript client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way. • snmp—An SNMP set request started the operation. • button—The CONFIG button on the router was pressed to commit the rescue configuration (if set) or to clear all configurations except the factory configuration. • autoinstall—Autoinstallation was performed. • other—Another method was used to commit the configuration.
Comment	Comment.
Log Message	<p>Method used to edit the configuration:</p> <ul style="list-style-type: none"> • Imported via paste—Configuration was edited and loaded with the Configuration>View and Edit>Edit Configuration Text option. For more information, see “CLI Editor (Edit Configuration Text)” on page 29. • Imported upload [filename]—Configuration was uploaded with the Configuration>View and Edit>Upload Configuration File option. For more information, see “Upload Configuration File” on page 90. • Modified via quick-configuration—Configuration was modified with the J-Web Quick Configuration tool specified by <i>quick-configuration</i>. • Rolled back via user-interface—Configuration was rolled back to a previous version through the user interface specified by <i>user-interface</i>, which can be Web Interface or CLI. For more information, see “Loading a Previous Configuration File” on page 88.
Action	Action to perform with the configuration file. The action can be Download or Rollback . For more information, see “Downloading a Configuration File” on page 89 and “Loading a Previous Configuration File” on page 88 .

For more information about saved versions of configuration files, see [“Editing and Committing a Junos OS Configuration” on page 35](#).

Displaying Users Editing the Configuration

To display a list of users editing the routing platform configuration, select **Maintain>Config Management>History**. The list is displayed as Database Information in the main pane (see [Figure 25 on page 88](#)). [Table 32 on page 88](#) summarizes the Database Information display.

Figure 25: Database Information Page

History						
Database Information						
The following users are editing the configuration:						
User Name	Start Time	Idle Time	Terminal	PID	Edit Flags	Edit Path
rob	2007-01-31 19:18:37 PST	16:16:14	p1	3423	None	[edit]
joe	2007-02-22 02:58:45 PST	13:56:25	p0	2962	None	[edit]
Configuration History						
The following table shows the router's commit history.						
To view a configuration, click the revision number.						

Table 32: J-Web Configuration Database Information Summary

Field	Description
User Name	Name of user editing the configuration.
Start Time	Time of day the user logged in to the routing platform.
Idle Time	Elapsed time since the user issued a configuration command from the CLI.
Terminal	Terminal on which the user is logged in.
PID	Process identifier assigned to the user by the routing platform.
Edit Flags	Designates a private or exclusive edit.
Edit Path	Level of the configuration hierarchy that the user is editing.

Loading a Previous Configuration File

To load (roll back) and commit a previous configuration file stored on the routing platform:

1. In the Action column, click **Rollback** for the version of the configuration you want to load.

The main pane displays the results of the rollback operation.



NOTE: When you click **Rollback**, the routing platform loads and commits the selected configuration. This behavior is different from entering the **rollback configuration mode** command from the CLI, where the configuration is loaded, but not committed.

Downloading a Configuration File

To download a configuration file from the routing platform to your local system:

1. In the Action column, click **Download** for the version of the configuration you want to download.
2. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

Comparing Configuration Files

To compare any two of the past 50 committed configuration files:

1. Click two of the check boxes to the left of the configuration versions you want to compare.
2. Click **Compare**.

The main pane displays the differences between the two configuration files at each hierarchy level as follows (see [Figure 26 on page 90](#)):

- Lines that have changed are highlighted side by side in green.
- Lines that exist only in the more recent configuration file are displayed in red on the left.
- Lines that exist only in the least recent configuration file are displayed in blue on the right.

Figure 26: J-Web Configuration File Comparison Results

History**Compare Rollback 5 Configuration to Rollback 2 Configuration**

Rollback 5 Configuration

[\[edit\]](#)

```
version 9.1B2.8;
```

Rollback 2 Configuration

[\[edit\]](#)

```
version "9.410 [builder]";
system {
  domain-name englab.juniper.net;
  domain-search [ englab.juniper.net juniper.net jnpr.net spglab.juniper.net ];
  backup-router 10.209.63.254;
  services {
    rlogin;
    rsh;
    ssh;
    telnet;
    web-management {
      http;
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 10.209.63.254;
  }
}
```

Legend:

Removed from Rollback 5 Configuration

changed lines

Added in Rollback 2 Configuration

Upload Configuration File

To upload a configuration file from your local system:

1. Select **Maintain>Config Management>Upload**.
The main pane displays the File to Upload box (see [Figure 27 on page 91](#)).
2. Specify the name of the file to upload using one of the following methods:
 - Type the absolute path and filename in the File to Upload box.
 - Click **Browse** to navigate to the file.
3. Click **Upload and Commit** to upload and commit the configuration.

The routing platform checks the configuration for the correct syntax before committing it.

Figure 27: J-Web Upload Configuration File Page

Config Management

Upload

Type the name of a configuration file on the local hard drive. When you click "Upload and Commit", the configuration in the file replaces the existing configuration and takes effect. If any errors occur when the file is loaded, configuration is restored.

• File to Upload ?

Using Rescue (J Series Routing Platforms Only)

If someone inadvertently commits a configuration that denies management access to a routing platform, you can delete the invalid configuration and replace it with a rescue configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI. The rescue configuration is a previously committed, valid configuration.

To view, set, or delete the rescue configuration, select **Maintain > Rescue**. On the Rescue page (see [Figure 28 on page 91](#)), you can perform the following tasks:

- View the current rescue configuration (if one exists)—Click **View rescue configuration**.
- Set the current running configuration as the rescue configuration—Click **Set rescue configuration**. On a J Series routing platform, you can also press the **CONFIG** or **RESET CONFIG** button.
- Delete the current rescue configuration—Click **Delete rescue configuration**.

Figure 28: Rescue Configuration Page

Rescue

If you inadvertently commit a configuration that denies management access, the only recourse may be to connect the console. The rescue configuration gives you another alternative. The rescue configuration is a configuration you know will allow management access to the router.

Press and immediately release the Config button on the chassis to cause the router to load and commit the rescue configuration. This will put the router back into a manageable state. You must have set the rescue configuration for this feature to function properly.

View Rescue Configuration

The rescue configuration for the router has been set. To view the rescue configuration, click the link below.

[View rescue configuration](#)

Set or Delete Rescue Configuration

Clicking 'Set rescue configuration' will set the rescue configuration to the current running configuration of the router. Clicking 'Delete rescue configuration' will delete the rescue configuration.

[Set rescue configuration](#)

[Delete rescue configuration](#)

Using Files

Select **Maintain>Files** in the J-Web interface to manage log, temporary, and core files on the routing platform.

[Table 33 on page 92](#) lists the different tasks that you can perform from the **Maintain>Files** page.

Table 33: Manage Files Tasks Summary

Manage Files Task	Functions
Clean Up Files	<p>Rotate log files and delete unnecessary files on the routing platform. If you are running low on storage space, the file cleanup procedure quickly identifies files that can be deleted.</p> <p>The file cleanup procedure performs the following tasks. Click Clean Up Files to begin.</p> <ul style="list-style-type: none"> • 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. <p>Alternatively, you can rotate log files and display the files that you can delete by entering the request system storage cleanup command at the J-Web CLI terminal. For more information, see “Using the CLI Terminal” on page 32. For more information about the request system storage cleanup command, see the Junos OS System Basics and Services Command Reference.</p>
Download and Delete Files	<p>Download a copy of an individual file or delete it from the routing platform. When you download a file, it is not deleted from the file system. When you delete the file, it is permanently removed.</p> <p>Click one of the following file types, and then select whether to download or delete a file:</p> <ul style="list-style-type: none"> • 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. • Old Junos OS—Lists the existing Junos OS packages in the /cf/var/sw directory on the router. • Crash (Core) Files—Lists the core files located in the /cf/var/crash directory on the router. <p>CAUTION: If you are unsure whether to delete a file from the router, we recommend using the Clean Up Files task, which determines the files that can be safely deleted from the file system.</p>
Delete Backup Junos Package	<p>Delete a backup copy of the previous software installation from the routing platform. When you delete the file, it is permanently removed from the file system.</p> <p>Click Delete backup Junos Package to begin.</p>

PART 4

Troubleshooting

- [J-Web User Interface on page 95](#)
- [Events on page 97](#)
- [Network on page 99](#)

CHAPTER 13

J-Web User Interface

- [Lost Router Connectivity on page 95](#)
- [Unpredictable J-Web Behavior on page 95](#)
- [No J-Web Access on page 95](#)

Lost Router Connectivity

- Problem** After completing initial configuration, I lost connectivity to the routing platform through J-Web.
- Cause** For J Series routers only, after initial configuration is complete, the routing platform stops functioning as a Dynamic Host Configuration Protocol (DHCP) server. If you change the IP address of the management interface and have the management device configured to use DHCP, you lose your DHCP lease and your connection to the routing platform through the J-Web interface.
- Solution** To reestablish a connection, either set the IP address on the management device manually, or connect the management interface to the management network and access the routing platform another way—for example, through the console port.

Unpredictable J-Web Behavior

- Problem** I have multiple J-Web windows open and am experiencing unpredictable results.
- Solution** Close the extra windows. The routing platform can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web windows—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

No J-Web Access

- Problem** I cannot access J-Web from my browser.
- Solution** **Solution 1**—On an M Series or T Series router, verify that you have successfully installed the J-Web software package and enabled Web management on the platform, as described in [“Installing the J-Web Software” on page 11](#).

Solution 2—If the routing platform is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the **Use SSL 3.0** option in the Web browser to access J-Web on the routing platform.

CHAPTER 14

Events

- Troubleshooting Events on page 97

Troubleshooting Events

Problem My View Events page does not display any events. (See [Figure 29 on page 97](#).)

Figure 29: View Events Page Displaying Error

The screenshot shows the 'View Events' page in the Junos J-Web interface. It features an 'Events Filter' section with the following fields: 'System Log File' (set to 'messages'), 'Process' (empty), 'Include archived files' (unchecked), 'Date From' (2009-07-17,03:54), 'To' (2009-07-17,04:54), 'Event ID' (empty), and 'Description' (empty). There are 'Search' and 'Reset' buttons. Below the filter is an 'Events Detail' section with a 'Generate Report' button. A table with columns 'Process', 'Severity', 'Event ID', 'Event Description', and 'Time' is shown, but it contains the message 'No events match filter condition'.

Process	Severity	Event ID	Event Description	Time
No events match filter condition				

Cause Typically, events are not displayed when logging of messages is not enabled. You can enable system log messages at a number of different levels using the J-Web configuration editor or the CLI terminal. The choice of level depends on how specific you want the event logging to be and what options you want to include. For details about the configuration options, see the [Junos OS System Basics Configuration Guide](#) (system level) or the [Junos OS Services Interfaces Configuration Guide](#) (all other levels).

Solution To enable system log messages with the J-Web configuration editor:

1. Navigate to **Configuration>View and Edit>Edit Configuration**.
2. Next to System, click **Configure** or **Edit** to navigate to the system level in the configuration hierarchy.
3. Next to Syslog, click **Configure** or **Edit** to navigate to the system log level in the configuration hierarchy.
4. Next to File, click **Add new entry** to create a log file.

5. In the File name box, type **messages** to name the log file.
6. Next to Contents, click **Add new entry** to select a facility that you want to configure—for example, **authorization**, **change-log**, **conflict-log**, or **user**.
7. In the Facility list, select **authorization** to configure the authorization facility.
8. In the Level list, select **info** to set the severity level to informational messages.
9. Repeat Steps 4 and 5 to configure different facilities and their levels.
10. To verify the configuration, at the CLI terminal, enter the **show syslog** command in configuration mode. (See [Figure 30 on page 98](#).)

Figure 30: Verifying System Log Messages Configuration

```
CLI Terminal
-----
A Java applet will be loaded below that will provide an SSH connection between your browser and '10.204.92.13'. You will be asked to enter your password again as a security measure before the CLI console connection is made. If the connection cannot be made, there may be a firewall between your web client and the device blocking SSH traffic, or you may be using a web proxy server which will allow web traffic to the device, but will not forward SSH traffic.

--- JUNOS 9.3R2.8 built 2008-12-17 23:25:33 UTC
% cli
regress@jotter> configure
Entering configuration mode

[edit]
regress@jotter# edit system

[edit system]
regress@jotter# show syslog
file messages {
    any notice;
    authorization info;
    kernel info;
    pfe info;
    archive world-readable;
}

[edit system]
regress@jotter# █
```

CHAPTER 15

Network

- [Using Ping Host on page 99](#)
- [Using Ping MPLS on page 100](#)
- [Using Ping ATM \(M Series, MX Series, and T Series Routing Platforms Only\) on page 101](#)
- [Using Traceroute on page 102](#)
- [Using Packet Capture on page 102](#)
- [Sample Task—Ping Host on page 102](#)

Using Ping Host

Use the Ping Host page to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The routing platform sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to a specified host to determine:

- Whether a remote host is active or inactive
- The round-trip delay in communicating with the host
- Packet loss

Entering a hostname or address on the Ping Host page creates a periodic ping task that runs until canceled or until it times out as specified. When you use the ping host tool, the routing platform first sends an echo request packet to an address, then waits for a reply. The ping is successful if it has the following results:

- The echo request gets to the destination host.
- The destination host is able to get an echo reply back to the source within a predetermined time called the round-trip time.

Alternatively, you can enter the **ping** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the **ping** command, see the *Junos OS System Basics and Services Command Reference*.

Because some hosts are configured not to respond to ICMP echo requests, a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you might find that you are not able to ping outside your local network.

Using Ping MPLS

Use the Ping MPLS page to diagnose the state of label-switched paths (LSPs), Layer 2 and Layer 3 virtual private networks (VPNs), and Layer 2 circuits. You can ping an MPLS endpoint using various options. You can send variations of ICMP echo request packets to the specified MPLS endpoint.

When you use the ping MPLS task from a Junos OS operating as the inbound (ingress) node at the entry point of an LSP or VPN, the routing platform sends probe packets into the LSP or VPN. Based on how the LSP or VPN outbound (egress) node at the remote endpoint of the connection replies to the probes, you can determine the connectivity of the LSP or VPN.

Each probe is an echo request sent to the LSP or VPN exit point as an MPLS packet with a UDP payload. If the outbound node receives the echo request, it checks the contents of the probe and returns a value in the UDP payload of the response packet. If the Junos OS receives the response packet, it reports a successful ping response.

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

[Table 34 on page 100](#) lists the ping MPLS tasks, summarizes their functions, and identifies corresponding CLI **show** commands you can enter at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 32](#).

Table 34: Ping MPLS Tasks Summary and the Corresponding CLI show Commands

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping RSVP-signaled LSP	ping mpls rsvp	Checks the operability of an LSP that has been set up by the Resource Reservation Protocol (RSVP). The Junos OS pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the Junos OS sends the ping requests on the path that is currently active.
Ping LDP-signaled LSP	ping mpls ldp	Checks the operability of an LSP that has been set up by the Label Distribution Protocol (LDP). The Junos OS pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the Junos OS sends the ping requests through the first gateway. Ping requests sent to LDP-signaled LSPs use only the master routing instance.
Ping LSP to Layer 3 VPN prefix	ping mpls l3vpn	Checks the operability of the connections related to a Layer 3 VPN. The Junos OS tests whether a prefix is present in a provider edge (PE) router's VPN routing and forwarding (VRF) table, by means of a Layer 3 VPN destination prefix.	The Junos OS does not test the connection between a PE router and a customer edge (CE) router.

Table 34: Ping MPLS Tasks Summary and the Corresponding CLI show Commands (*continued*)

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping LSP for a Layer 2 VPN connection by interface	ping mpls l2vpn interface	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS directs outgoing request probes out the specified interface.	For information about interface names, see the Junos OS Interfaces Command Reference .
Ping LSP for a Layer 2 VPN connection by instance	ping mpls l2vpn instance	Checks the operability of the connections related to a Layer 2 VPN. The Junos OS pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, to test the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound and outbound PE routers.	
Ping LSP to a Layer 2 circuit remote site by interface	ping mpls l2circuit interface	Checks the operability of the Layer 2 circuit connections. The Junos OS directs outgoing request probes out the specified interface.	
Ping LSP to a Layer 2 circuit remote site by VCI	ping mpls l2circuit virtual-circuit	Checks the operability of the Layer 2 circuit connections. The Junos OS pings on a combination of the IPv4 prefix and the virtual circuit identifier on the outbound PE router, testing the integrity of the Layer 2 circuit between the inbound and outbound PE routers.	
Ping end point of LSP	ping mpls lsp-end-point	Checks the operability of an LSP endpoint. The Junos OS pings an LSP endpoint using either an LDP FEC prefix or an RSVP LSP endpoint address.	

Using Ping ATM (M Series, MX Series, and T Series Routing Platforms Only)

On M Series, MX Series, and T Series routers, use the Ping ATM pages to ping an Asynchronous Transfer Mode (ATM) node on an ATM virtual circuit (VC) pathway to verify that the node can be reached over the network. The output is useful for diagnosing ATM node and network connectivity problems. The routing platform sends a series of echo requests to a specified ATM node and receives echo responses.

Alternatively, you can enter the **ping atm** command at the J-Web CLI terminal. For more information, see “[Using the CLI Terminal](#)” on page 32. For more information about the **ping atm** command, see the [Junos OS System Basics and Services Command Reference](#).

Using Traceroute

Use the Traceroute page to trace a route between the routing platform and a remote host. You can use the traceroute task to display a list of routers between the routing platform and a specified destination host. The output is useful for diagnosing a point of failure in the path from the routing platform to the destination host, and addressing network traffic latency and throughput problems.

The routing platform generates the list of routers by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive router is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each router along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The routing platform sends a total of three traceroute packets to each router along the path and displays the round-trip time for each traceroute operation. If the routing platform times out before receiving a **Time Exceeded** message, an asterisk (*) is displayed for that round-trip time.

Alternatively, you can enter the **traceroute** command at the J-Web CLI terminal. For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the **traceroute** command, see the *Junos OS System Basics and Services Command Reference*.

Using Packet Capture

Use the Packet Capture page when you need to quickly capture and analyze router control traffic on a routing platform. The Packet Capture page allows you to capture traffic destined for or originating from the Routing Engine. You can use the packet capture task to compose expressions with various matching criteria to specify the packets that you want to capture. You can either choose to decode and view the captured packets in the J-Web interface as they are captured, or save the captured packets to a file and analyze them offline with packet analyzers such as Ethereal. The packet capture task does not capture transient traffic.

Alternatively, you can use the CLI **monitor traffic** command at the J-Web CLI terminal to capture and display packets matching a specific criteria. For more information, see [“Using the CLI Terminal” on page 32](#). For more information about the **monitor traffic** command, see the *Junos OS System Basics and Services Command Reference*.

To capture transient traffic and entire IPv4 data packets for offline analysis, you must configure packet capture with the J-Web or CLI configuration editor. For details, see the *J-series Services Router Administration Guide*.

Sample Task—Ping Host

[Figure 31 on page 103](#) shows a sample Ping Host page. In this example, you are sending ping requests to two destination hosts—**10.10.2.2** and **10.10.10.10**. The echo requests reaches **10.10.2.2** and does not reach **10.10.10.10**.

To ping the host:

1. Select **Troubleshoot>Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon (see [Figure 31 on page 103](#)).
3. Next to Remote Host, type **10.10.2.2** to specify the host's IP address.
4. Retain the default values in the following fields:
 - Interface—**any**—Ping requests to be sent on all interfaces.
 - Count—**10**—Number of ping requests to send.
 - Type-of-Service—**0**—TOS value in the IP header of the ping request packet.
 - Routing Instance—**default**—Routing instance name for the ping attempt.
 - Interval—**1**—Interval, in seconds, between the transmission of each ping request.
 - Packet Size—**56**—Size of the ping request packet in bytes. The routing platform adds 8 bytes of ICMP header to this size before sending it.
 - Time-to-Live—**32**—TTL hop count for the ping request packet.
5. Click **Start**.
6. Repeat Steps 2 through 5 to ping destination host **10.10.10.10**.

Figure 31: Ping Host Troubleshoot Page

Ping Host

Ping Host

The ping diagnostic tool sends a series of ICMP "echo request" packets to the specified remote host.

The receipt of such packets will usually result in the remote host replying with an ICMP "echo response." Note that some hosts are configured not to respond to ICMP "echo requests," so a lack of responses does not necessarily represent a connectivity problem. Also, some firewalls block the ICMP packet types that ping uses, so you may find that you are not able to ping outside your local network.

Entering a host below creates a periodic ping task that will run until cancelled or until it times out as specified.

* Remote Host ?

☐ **Advanced options**

Don't Resolve Addresses <input type="checkbox"/> ?	Routing Instance <input type="text" value="default"/> ?
Interface <input type="text" value="any"/> ?	Interval <input type="text" value="1"/> ?
Count <input type="text" value="10"/> ?	Packet Size <input type="text" value="56"/> ?
Don't Fragment <input type="checkbox"/> ?	Source Address <input type="text"/> ?
Record Route <input type="checkbox"/> ?	Time-to-Live <input type="text" value="32"/> ?
Type-of-Service <input type="text" value="0"/> ?	Bypass Routing <input type="checkbox"/> ?

[Figure 32 on page 104](#) displays the results of a successful ping in the main pane, and [Table 35 on page 104](#) provides a summary of the ping host results and output.

Figure 32: Successful Ping Host Results Page

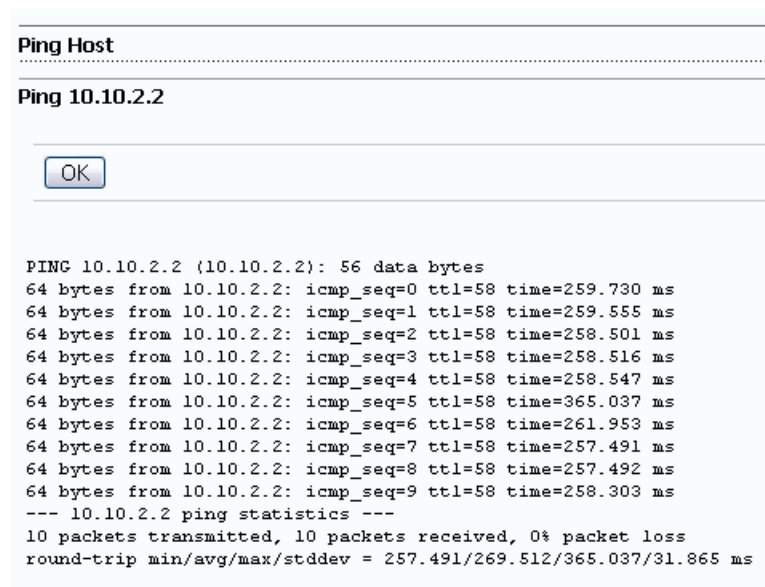


Table 35: J-Web Ping Host Results and Output Summary

Ping Host Result	Description
64 bytes from	Size of ping response packet, which is equal to the default value in the Packet Size box (56), plus 8.
10.10.2.2	IP address of the destination host that sent the ping response packet.
icmp_seq= <i>number</i>	Sequence numbers of packets from 0 through 9. You can use this value to match the ping response to the corresponding ping request.
ttl=58	Time-to-live hop-count value of the ping response packet.
259.730 ms	Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
10 packets transmitted, 10 packets received, 0% packet loss	Ping packets transmitted, received, and lost. 10 ping requests (probes) were sent to the host, and 10 ping responses were received from the host. No packets were lost.
257.491/269.512/365.037/31.865 ms	<ul style="list-style-type: none"> 257.491—Minimum round-trip time 269.512—Average round-trip time 365.037—Maximum round-trip time 31.865—Standard deviation of the round-trip times ms—milliseconds

Figure 33 on page 105 shows the output of an unsuccessful ping. There can be different reasons for an unsuccessful ping. This result shows that the local router did not have a route to the host 10.10.10.10 and thus could not reach it.

Figure 33: Unsuccessful Ping Host Results Page

Ping Host

Ping 10.10.10.10

OK

```

PING 10.10.10.10 (10.10.10.10): 56 data bytes
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 3825 0 0000 1a 01 411f 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 383e 0 0000 1a 01 4106 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable
Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
 4 5 00 0054 384f 0 0000 1a 01 40f5 10.209.8.129 10.10.10.10
36 bytes from 172.28.2.194: Destination Net Unreachable

```


PART 5

Index

- [Index on page 109](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
* (red asterisk).....	6
/cf/var/crash directory See crash files	
/cf/var/log directory See system logs	
/cf/var/tmp directory See temporary files	
< >, in syntax descriptions.....	xiv
? icon	6
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

access, configuration summary.....	25
accounting options	
configuration summary.....	25
sample task.....	40
Add new entry link.....	38
advanced BGP feature, license.....	64
alarms	
chassis.....	52
interface.....	52
major.....	52
minor.....	52
red.....	52
severity.....	52
system.....	52
type.....	52
viewing, sample.....	53
yellow.....	52
alarms sample task.....	53
alert logging severity.....	57
applications, configuration summary.....	25

B

backup	
boot device.....	65
current configuration.....	65
rescue configuration.....	65
system software.....	65

basic connectivity	
Quick Configuration.....	14
requirements.....	14
selecting.....	67
braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv
browser interface See J-Web interface	
buttons	
Cancel (J-Web configuration editor).....	8, 39
Commit (J-Web configuration editor).....	8, 39
Discard (J-Web configuration editor).....	39
OK (J-Web configuration editor).....	8, 39
Refresh (J-Web configuration editor).....	39

C

Cancel button.....	39
J-Web configuration editor.....	8
certificates See SSL certificates	
chassis	
configuration summary.....	26
monitoring.....	79
chassis viewer.....	70
class of service (CoS)	
configuration summary.....	26
monitoring.....	71
cleaning up files.....	92
CLI See Junos OS CLI	
CLI terminal.....	32
overview.....	32
starting.....	31
clickable configuration See J-Web configuration editor	
command-line interface See Junos OS CLI	
comments, in configuration statements.....	xiv
Commit button.....	8, 39
committed configuration	
comparing two configurations.....	89
methods.....	87
overview.....	23, 35
rescue configuration	91
storage location.....	24, 35
summaries.....	86
committing a configuration.....	23, 35
configuration	
committing	39
committing as a text file, with caution	29
discarding changes	39

downloading	89	Discard button.....	39
editing	25, 36	Discard Changes Below This Point option	
editing as a text file, with caution	29	button.....	40
loading previous	88	discarding configuration changes.....	39
rollback	88	DNS server, defining (Quick Configuration).....	16
uploading	90	documentation	
users-editors, viewing.....	87	comments on.....	xiv
viewing as a text file	28	domain name, defining (Quick Configuration).....	15
configuration database, summary.....	88	domain search, defining (Quick Configuration).....	16
configuration hierarchy, J-Web display.....	7	downgrading Junos OS.....	63
configuration history		downloading configuration files	89
comparing files.....	89		
database summary.....	88	E	
downloading files.....	89	Edit Configuration page.....	37
summary.....	86	Edit Configuration Text page.....	29
users-editors, viewing.....	87	edit link.....	38
Configuration History page.....	86	editing a configuration.....	25
configuration sample tasks		emergency logging severity.....	57
accounting options.....	40	error logging severity.....	57
configuration text		event options, configuration summary.....	26
editing and committing, with caution.....	29	events	
viewing.....	28	filtering.....	57
configure link.....	38	filters.....	57
connectivity		overview.....	55
losing, after initial configuration.....	95	regular expressions for filtering.....	59
lost DHCP lease after initial configuration.....	15	severity levels.....	57
conventions		using.....	55
text and syntax.....	xiii	viewing.....	56
CoS See class of service		viewing, sample.....	60
crash files, cleaning up.....	92	events sample task.....	60
critical logging severity.....	57		
curly braces, in configuration statements.....	xiv	F	
customer support.....	xv	fe-0/0/0, defining address (Quick	
contacting JTAC.....	xv	Configuration).....	17
D		feature licenses See license	
data link switching (DLSw), license.....	64	file management	
Database Information page.....	86	crash files	92
debug logging severity.....	57	log files	92
default gateway		temporary files	92
defining (Quick Configuration).....	16	filtering events	
Delete Configuration Below This Point option		overview.....	57
button.....	40	regular expressions.....	59
delete link.....	38	firewall filters	
deleting a current rescue configuration	91	configuration summary.....	26
DHCP (Dynamic Host Configuration Protocol)		monitoring.....	76
monitoring.....	78	sample task.....	60
DHCP server, regaining lost lease.....	15, 95	font conventions.....	xiii
Discard All Changes option button.....	40	Forwarding Engine Board redundancy	
		monitoring.....	80

forwarding options, configuration summary.....26
 fxp0, defining address (Quick Configuration).....17

G

ge-0/0/0, defining address (Quick Configuration).....17

H

halting a Services Router immediately.....67
 hardware, major (red) alarm conditions on.....52
 Help icon (?).....6, 8
 Help, J-Web interface.....4, 8
 hostname, defining (Quick Configuration).....15
 HTTP (Hypertext Transfer Protocol)
 enabling Web access.....47
 on built-in management interfaces.....19
 httpd process, limiting subordinate processes.....45
 HTTPS (Hypertext Transfer Protocol over SSL)
 enabling secure access.....47
 recommended for secure access.....19
 Hypertext Transfer Protocol See HTTP
 Hypertext Transfer Protocol over SSL See HTTPS

I

identifier link.....38
 info logging severity.....57
 initial configuration requirements.....14
 installing Junos OS.....63
 interfaces
 configuration summary.....26
 monitoring.....72
 Internet Explorer, modifying for worldwide version
 of Junos OS.....12
 invalid configuration, replacing.....91
 IPsec tunnels
 monitoring.....77

J

J-Web configuration editor
 committing a configuration.....39
 configuration hierarchy display.....7
 configuration text, viewing.....28
 editing a configuration.....36
 J-Web interface
 comparing configuration differences.....89
 context-sensitive help.....4
 event viewer.....60
 Help (?) icon.....6

Internet Explorer, modifying for worldwide
 version of Junos OS.....12
 layout.....4
 losing connectivity after initial
 configuration.....95
 main pane.....5
 overview.....3, 23
 page layout.....4
 side pane.....6
 starting.....12
 top pane.....4
 unpredictable results, multiple windows.....95

J-Web Quick Configuration See Quick Configuration

J-Web software, installing.....11

Junos OS

downgrading.....63
 installing.....63
 Internet Explorer, modifying for worldwide
 version.....12
 upgrading.....63
 worldwide version, modifying Internet Explorer
 for.....12

Junos OS CLI.....32
 command modes.....32
 overview.....32
 See also CLI terminal

JUNOScript

 enabling secure access.....47

JUNOScript API

 defining access (Quick Configuration).....17

JUNOScript over SSL.....47

L

layout, J-Web.....4
 license

 add.....64
 advanced BGP feature.....64
 data link switching (DLSw).....64
 delete.....64
 display keys.....64
 manage.....64

limitations

 software downgrade cannot be undone.....64
 unpredictable behavior with multiple
 windows.....95

loading a configuration file

 downloading89
 rollback88
 uploading90

logging severity levels.....	57
loopback address, defining (Quick Configuration).....	16

M

main pane, J-Web.....	5
major (red) alarms.....	52
Management Access page	
description.....	47
management device	
monitoring from.....	69
management interface address, defining (Quick Configuration).....	17
manuals	
comments on.....	xiv
minor (yellow) alarms.....	52
monitor sample task.....	81, 82
monitoring	
chassis.....	79
chassis viewer.....	70
class of service.....	71
CLI commands and corresponding J-Web options.....	69
DHCP.....	78
FEB redundancy.....	80
firewall filters.....	76
interfaces.....	72
interfaces, sample.....	81
IPsec.....	77
J-Web tasks and corresponding CLI commands.....	69
MPLS.....	73
NAT.....	77
overview.....	69
<i>See also</i> diagnosis; statistics; status	
PPPoE.....	74
Process Details.....	80
route information, sample.....	82
routing.....	75
RPM.....	74
service sets.....	78
system.....	79
MPLS, monitoring.....	73

N

NAT (Network Address Translation)	
monitoring.....	77
Network Address Translation <i>See</i> NAT	
network connectivity.....	99

notice logging severity.....	57
NTP server, defining (Quick Configuration).....	16

O

OK button.....	39
J-Web configuration editor.....	8
openssl command.....	19
option buttons	
Delete Configuration Below This Point.....	40
Discard All Changes.....	40
Discard Changes Below This Point.....	40

P

packet capture.....	102
pages, layout in J-Web.....	4
parentheses, in syntax descriptions.....	xiv
partition, storage medium.....	65
ping	
ATM.....	101
host.....	99
MPLS.....	100
ping host	
results.....	104
sample.....	102
Ping LSP for a Layer 2 VPN connection by interface.....	101
Ping LSP to a Layer 2 circuit remote site by VCI.....	101
ping MPLS	
layer-2 VPN, instance.....	100
layer-2 VPN, interface.....	100
LDP-signaled LSP.....	100
LSP endpoint.....	100
LSP to Layer 3 VPN prefix.....	100
options.....	36
RSVP-signaled LSP.....	100
policy options, configuration summary.....	26
PPPoE, monitoring.....	74
Process Details	
monitoring.....	80

Q

Quick Configuration	
basic settings.....	14
initial configuration.....	14

R

real-time performance monitoring <i>See</i> RPM	
reboot immediately	67
red asterisk (*).....	6

Refresh button.....	39
regaining DHCP lease after initial configuration.....	15
regular expressions for filtering events.....	59
required entry	6
rescue configuration	
deleting	91
setting	91
viewing	91
rolling back a configuration file during	
configuration.....	88
root password, defining (Quick Configuration).....	15
route information sample task.....	82
routing instances, configuration summary.....	27
routing options, configuration summary.....	27
routing protocols	
configuration summary.....	27
routing, monitoring.....	75
RPM (real-time performance monitoring)	
graph results.....	75
monitoring.....	74
RPM probes.....	75
sample graphs.....	75

S

sample tasks	
configuring accounting options.....	40
filtering and viewing events.....	60
managing snapshots.....	66
monitoring interfaces.....	81
monitoring route information.....	82
ping host.....	102
viewing alarms.....	53
scheduling a reboot.....	67
secure access	
generating SSL certificates.....	19
HTTPS access.....	47
HTTPS recommended.....	19
installing SSL certificates.....	47
JUNOScript SSL access.....	47
Secure Access page	
description.....	47
field summary.....	48
security, configuration summary.....	27
service sets, monitoring.....	78
services, configuration summary.....	27
sessions	
limiting number of.....	45
limits.....	45
terminating.....	46
Set Up page	
field summary.....	15
prerequisites.....	14
setup	
Quick Configuration.....	14
requirements.....	14
severity levels for events.....	57
side pane, J-Web.....	6
snapshot	
sample task.....	66
system software.....	65
SNMP	
configuration summary.....	27
software package	
downgrading.....	63
installing.....	63
upgrading.....	63
software, halting immediately.....	67
SSH, defining access (Quick Configuration).....	17
SSL (Secure Sockets Layer)	
enabling secure access.....	47
SSL 3.0 option, disabling on Internet Explorer for	
worldwide version of Junos OS.....	12
SSL certificates	
adding (Quick Configuration).....	48
generating.....	19
startup, J-Web interface.....	12
support, technical See technical support	
syntax conventions.....	xiii
system	
configuration summary.....	27
monitoring.....	79
system log messages	
displaying at a terminal (configuration	
editor).....	59
filtering.....	57
overview.....	55
system logs	
enabling.....	97
file cleanup	92
functions.....	55
logging severity levels.....	57
messages See system log messages	
system management	
files.....	92
licenses.....	64
reboots.....	67
software.....	63

system time	
defining (Quick Configuration).....	16
synchronizing (Quick Configuration).....	16

T

taskbar.....	5
technical support	
contacting JTAC.....	xv
Telnet, defining access (Quick Configuration).....	17
temporary files, cleaning up.....	92
time to live <i>See</i> TTL	
time zone, defining (Quick Configuration).....	16
timeout sessions.....	45
top pane, J-Web.....	4
traceroute, overview.....	102
troubleshoot	
CLI terminal.....	32
network connectivity.....	99
packet capture.....	102
ping ATM.....	101
ping host.....	99
ping MPLS.....	100
traceroute.....	102
troubleshoot sample task.....	102
troubleshooting	
events.....	97
J-Web access.....	95
J-Web behavior.....	95
router connectivity.....	95
TTL (time to live), ping requests.....	104

U

unknown logging severity.....	57
upgrading Junos OS.....	63
uploading a configuration file.....	90
user interfaces	
preparation.....	12
users	
viewing.....	46
using alarms tasks.....	51

V

view and edit	
committing a text file, with caution.....	29
configuration text, viewing.....	28
configuration, editing.....	25
uploading a file.....	90
View Configuration Text page.....	28

View Events page	
field summary (filtering log messages).....	58
overview.....	55
viewing alarms, sample task.....	53
viewing configuration text.....	28
viewing events, sample task.....	60

W

warning logging severity.....	57
Web access, secure <i>See</i> secure access	
Web browser, modifying Internet Explorer for	
worldwide version of Junos OS.....	12
windows, J-Web, unpredictable results with	
multiple.....	95

Y

yellow alarms.....	52
--------------------	----