



JUNOS™ Software

J-Web Interface User Guide

Release 9.5

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-029756-01, Revision 1

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

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

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

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

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

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

JUNOS™ Software J-Web Interface User Guide

Release 9.5

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Philomena Dolla and Preeti Karkera

Editing: Nancy Kurahashi

Illustration: Faith Bradford Brown and Nathaniel Woodward

Cover Design: Edmonds Design

Revision History

13 April 2009—530-029756-01 Revision 1

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

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Abbreviated Table of Contents

	About This Guide	xiii
Part 1	Introduction to J-Web	
Chapter 1	Installing, Starting, and Managing J-Web	3
Chapter 2	J-Web User Interface Overview	17
Part 2	J-Web Tasks	
Chapter 3	Monitor Tasks	27
Chapter 4	Configuration Tasks	43
Chapter 5	Diagnose Tasks	73
Chapter 6	Manage Tasks	85
Chapter 7	Events Tasks	91
Chapter 8	Alarms Tasks (J-series Routing Platforms Only)	99
Part 3	Index	
	Index	105

Table of Contents

	About This Guide	xiii
	JUNOS Documentation and Release Notes	xiii
	Objectives	xiv
	Audience	xiv
	Supported Routing Platforms	xv
	How to Use This Guide	xv
	Document Conventions	xvi
	Documentation Feedback	xviii
	Requesting Technical Support	xviii
Part 1	Introduction to J-Web	
Chapter 1	Installing, Starting, and Managing J-Web	3
	Installing the J-Web Software	3
	Starting the J-Web Interface	4
	Configuring Basic Settings	6
	Secure Web Access Overview	9
	Generating SSL Certificates	9
	Configuring Secure Web Access	10
	Terminating J-Web Sessions	13
	Setting J-Web Session Limits	13
	Viewing Current Users	14
	Lost Router Connectivity	14
	Unpredictable J-Web Behavior	14
	No J-Web Access	14
Chapter 2	J-Web User Interface Overview	17
	J-Web Overview	17
	J-Web Layout	18
	Top Pane Elements	19
	Main Pane Elements	20
	Side Pane Elements	21
	Navigating the J-Web Interface	22
	Navigating the Quick Configuration Pages	22
	Navigating the J-Web Configuration Editor	22
	Getting J-Web Help	23

Part 2**J-Web Tasks****Chapter 3****Monitor Tasks****27**

Monitor Task Overview	27
System	28
Chassis	28
Interfaces	29
Routing	29
Class of Service	30
MPLS	31
Service Sets	32
Firewall	33
IPSec	33
NAT	34
DHCP (J-series Routing Platforms Only)	34
RPM	35
PPPoE (J-series Routing Platforms Only)	36
FEB Redundancy (M120 Routing Platforms Only)	36
Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only)	37
Sample Task—Monitoring Interfaces	38
Sample Task—Monitoring Route Information	40

Chapter 4**Configuration Tasks****43**

Configuration Task Overview	43
Editing and Committing a JUNOS Configuration	45
J-Web Configuration Tasks	46
Using Quick Configuration	47
Sample Task—Configuring Setup with Quick Configuration	49
Configuring the Router Identification	50
Configuring the Network	51
Configuring the Management Access	51
Sample Task—Configuring Firewall Filters with Quick Configuration	51
View Configuration Text	53
Edit Configuration Page (J-Web Configuration Editor)	55
Editing a Configuration	58
Discarding Parts of a Candidate Configuration	61
Committing a Configuration	62
Accounting Options	62
Edit Configuration Text	64
Upload Configuration File	65
Displaying Configuration History	66
Displaying Users Editing the Configuration	68
Comparing Configuration Files	69
Downloading a Configuration File	70
Loading a Previous Configuration File	71
Using Rescue (J-series Routing Platforms Only)	71

Chapter 5	Diagnose Tasks	73
	Using Ping Host	73
	Using Ping MPLS	74
	Using Ping ATM (M-series, MX-series, and T-series Routing Platforms only)	75
	Using Traceroute	76
	Using Packet Capture	76
	Using the CLI Terminal	77
	CLI Terminal Requirements	78
	Starting the CLI Terminal	79
	Sample Task—Ping Host	80
Chapter 6	Manage Tasks	85
	Using Files	85
	Using Software (J-series Routing Platforms Only)	86
	Using Licenses (J-series Routing Platform Only)	87
	Using Reboot	88
	Using Snapshot (J-series Routing Platforms Only)	89
	Sample Task—Manage Snapshots	90
Chapter 7	Events Tasks	91
	Using View Events	91
	Viewing Events	92
	Understanding Severity Levels	92
	Using Filters	93
	Using Regular Expressions	95
	Sample Task—Filtering and Viewing Events	96
	Troubleshooting Events	97
Chapter 8	Alarms Tasks (J-series Routing Platforms Only)	99
	Using Alarms	99
	Active Alarms Information	99
	Alarm Severity	100
	Displaying Alarm Descriptions	100
	Sample Task—Viewing and Filtering Alarms	100
Part 3	Index	
	Index	105

About This Guide

This preface provides the following guidelines for using the *JUNOS Software J-Web Interface User Guide*:

- JUNOS Documentation and Release Notes on page xiii
- Objectives on page xiv
- Audience on page xiv
- Supported Routing Platforms on page xv
- How to Use This Guide on page xv
- Document Conventions on page xvi
- Documentation Feedback on page xviii
- Requesting Technical Support on page xviii

JUNOS Documentation and Release Notes

For a list of related JUNOS documentation, see <http://www.juniper.net/techpubs/software/junos/>.

If the information in the latest *JUNOS Release Notes* differs from the information in the documentation, follow the *JUNOS Release Notes*.

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

Table 1 on page xiii lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 1: Additional Books Available Through <http://www.juniper.net/books>

Book	Description
<i>Interdomain Multicast Routing</i>	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.

Table 1: Additional Books Available Through <http://www.juniper.net/books> (continued)

Book	Description
<i>JUNOS Cookbook</i>	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
<i>MPLS-Enabled Applications</i>	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
<i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i>	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multipoint-to-multipoint routing; and covers troubleshooting for OSPF and IS-IS networks.
<i>Routing Policy and Protocols for Multivendor IP Networks</i>	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
<i>The Complete IS-IS Protocol</i>	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Objectives

This guide describes how to use the J-Web user interface to configure, monitor, and manage Juniper Networks routing platforms.

This guide is not directly related to any particular release of the JUNOS software. To obtain the most current version of this manual, refer to the product documentation page on the Juniper Networks Web site, which is located at <http://www.juniper.net>.

Juniper Networks routing platform operations are controlled by the JUNOS software. You can configure and manage the JUNOS software through either a command-line interface (CLI) or a Web browser called the J-Web user interface. The J-Web interface works with most Web browsers, including Microsoft Internet Explorer and Netscape Navigator. To use the J-Web interface, you must have access to a Web browser application on your system.

Audience

This guide is designed for individuals who prefer using a graphical user interface (GUI) for installing, configuring, and managing a Juniper Networks routing platform. The guide is intended for the following audiences:

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

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

Supported Routing Platforms

The J-Web user interface is supported on the following routing platforms running the JUNOS software:

- J-series
- M-series
- MX-series
- T-series

How to Use This Guide

This guide provides a comprehensive two-part overview of the J-Web user interface. Part 1 describes how to install and start the J-Web interface, explains its layout, and identifies the elements that comprise the interface. Part 2 describes the tasks you perform on a routing platform with the J-Web interface. The chapters describing J-Web tasks follow the order in which the tasks appear in the interface.

Although this guide does not include a description of each J-Web page, much of this information appears elsewhere in Juniper Networks documentation. See Table 2 on page xv for the location of J-Web information and [\[Unresolved xref\]](#) for a comprehensive list of documentation for routing platforms operating on the JUNOS software.

Table 2: Location of J-Web Information

J-Web Information	Location
How to install the J-Web interface.	“Installing, Starting, and Managing J-Web” on page 3
<ul style="list-style-type: none"> ■ J-Web layout and elements. ■ How to navigate the J-Web interface. 	“J-Web User Interface Overview” on page 17

Table 2: Location of J-Web Information *(continued)*

J-Web Information	Location
How to perform typical tasks—Monitor, Configuration, Diagnose, Manage, Events, Alarms—on your routing platform with the J-Web interface.	<ul style="list-style-type: none"> ■ Monitor Tasks on page 27 ■ Configuration Tasks on page 43 ■ Manage Tasks on page 85 ■ Diagnose Tasks on page 73 ■ Events Tasks on page 91 ■ Alarms Tasks (J-series Routing Platforms Only) on page 99
How to use each field on the Quick Configuration task pages and many fields on the View and Edit configuration task pages.	<ul style="list-style-type: none"> ■ J-Web Help (see “Getting J-Web Help” on page 23) ■ <i>J-series Services Router Basic LAN and WAN Access Configuration Guide</i> ■ <i>J-series Services Router Advanced WAN Access Configuration Guide</i>
How to use each field on the Monitor, Manage, Diagnose, Events, and Alarms task pages.	<ul style="list-style-type: none"> ■ J-Web Help (see “Getting J-Web Help” on page 23) ■ <i>J-series Services Router Administration Guide</i>

Document Conventions

Table 3 on page xvi defines the notice icons used in this guide.

Table 3: Notice Icons





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

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

Table 4: Text and Syntax Conventions

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

Table 4: Text and Syntax Conventions (*continued*)

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

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1

Introduction to J-Web

- Installing, Starting, and Managing J-Web on page 3
- J-Web User Interface Overview on page 17

Chapter 1

Installing, Starting, and Managing J-Web

- Installing the J-Web Software on page 3
- Starting the J-Web Interface on page 4
- Configuring Basic Settings on page 6
- Secure Web Access Overview on page 9
- Generating SSL Certificates on page 9
- Configuring Secure Web Access on page 10
- Terminating J-Web Sessions on page 13
- Setting J-Web Session Limits on page 13
- Viewing Current Users on page 14
- Lost Router Connectivity on page 14
- Unpredictable J-Web Behavior on page 14
- No J-Web Access on page 14

Installing the J-Web Software

Your routing platform comes with the JUNOS software installed on it. When you power on the routing platform, all software starts automatically. On J-series routing platforms, the J-Web software is part of the JUNOS software available by default. However, on M-series and T-series routing platforms 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 Web page 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 routing platforms must be running JUNOS software 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 software 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 software. 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 software and you are using the Microsoft Internet Explorer Web browser, you must disable the **Use SSL 3.0** option in the Web browser to access the 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 **Quick Configuration > Set Up** or **Monitor > System** 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 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 Quick Configuration:

1. Navigate to the Set Up Quick Configuration page by selecting **Configuration > Quick Configuration > Set Up** (see Figure 1 on page 7).
2. Enter information into the Set Up Quick Configuration page, as described in Table 5 on page 7.
3. Click **Apply** to apply the configuration.

Figure 1: J-Web Set Up Quick Configuration Page

Quick 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 routing platforms only, after initial configuration is complete, the routing platform stops functioning as a 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 5: Set Up Quick Configuration 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.

Table 5: Set Up Quick Configuration Summary (continued)

Field	Function	Your Action
Root Password (required)	Sets the root password that 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.
Verify Root Password (required)	Verifies 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.	To add an IP address, type it in the box to the left of the Add button, then click Add . To delete an IP address, click it in the box above the Add button, then click Delete .
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.	To add an IP address, type it in the box to the left of the Add button, then click Add . To delete an IP address, click it in the box above the Add button, then click Delete .
Domain Search	Adds each domain name that the router is included in to the configuration so that they are included in a DNS search.	To add a domain name, type it in the box to the left of the Add button, then click Add . To delete a domain name, click it in the box above the Add button, then click Delete .
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 5: Set Up Quick Configuration Summary (continued)

Field	Function	Your Action
fe-0/0/0 Address (on J2300, J4300 and J6300 routing platforms)	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 routing platforms)		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 routing platforms)		
Management Access		
Allow Telnet Access	Allows remote access to the router using Telnet.	To enable Telnet access, select the check box.
Allow JUNOScript over Clear-Text Access	Allows JUNOScript to access the router 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 using SSH.	To enable SSH access, select the check box.

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 routing platforms, 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 file `new.pem`.

```
cat new.pem
```

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

Go on to “Configuring Secure Web Access” on page 10 to install the SSL certificate and enable HTTPS.

Configuring Secure Web Access

Navigate to the Secure Access Quick Configuration page by selecting **Configuration > Quick Configuration > Secure Access**. 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 2 on page 11 shows the Secure Access Quick Configuration page.

Figure 2: Quick Configuration Secure Access Page

Quick Configuration

Secure Access

Certificates

Local certificates are used in providing SSL server access.

No certificates are defined.

[Add...](#)

HTTP Web Access

HTTP access allows management of the router via the web interface. Communication between the router web server and your browser is sent in the clear (including passwords!), so it is recommended that you do disallow HTTP access from your WAN interfaces.

Enable HTTP access ☒ ?

Enable HTTP on All Interfaces ☒

HTTP-Enabled Interfaces

HTTP Interfaces

Logical Interfaces

fe-0/0/0.0
lo0.0

HTTPS Web Access

HTTPS access allows secure management of the router via the web interface. Communication between the router web server and your browser is encrypted using a session key negotiated using the SSL server certificate.

Enable HTTPS access ☐ ?

* HTTPS Certificate ?

Enable HTTPS on All Interfaces ☒

HTTPS-Enabled Interfaces

HTTPS Interfaces

Logical Interfaces

fe-0/0/0.0
lo0.0

JUNOScript over SSL

Configuring SSL access for the JUNOScript XML scripting API access allows secure management of the router.

Enable SSL JUNOScript access ☐ ?

* JUNOScript SSL Certificate ?

[Apply](#)

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

1. Enter information into the Secure Access Quick Configuration page, as described in Table 6 on page 12.
2. Click **Apply** 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 JUNOScope is required. For information about how to log in to JUNOScope, see the *JUNOScope Software User Guide*.

Table 6: Secure Access Quick Configuration Summary

Field	Function	Your Action
Certificates		
Certificates	Displays digital certificates required for SSL access to the routing platform.	To add a certificate:
	Allows you to add and delete SSL certificates.	<ol style="list-style-type: none"> 1. Click Add. Opens the Add a Local Certificate page. 2. Type a name in the Certificate Name box—for example, new. 3. Paste the generated certificate and RSA private key in the Certificate box.
	For information about how to generate an SSL certificate, see “Generating SSL Certificates” on page 9.	
		To delete a certificate, select it and click Delete .
HTTP Web Access		
Enable HTTP Access	Enables HTTP access on interfaces.	To enable HTTP access, select the Enable HTTP access check box.
Enable HTTP on All Interfaces	Enables HTTP access on all interfaces at one time.	To enable HTTP access on all interfaces, select the Enable HTTP on All Interfaces check box.
HTTP-Enabled Interfaces	Specifies interfaces on which you want to enable HTTP access.	Select and deselect interfaces by clicking the direction arrows: <ul style="list-style-type: none"> ■ To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. ■ To disable HTTP access on an interface, add the interface to the Logical Interfaces list.
HTTPS Web Access		
Enable HTTPS Access	Enables HTTPS access on interfaces.	To enable HTTPS access, select the Enable HTTPS access check box.
HTTPS Certificate	Specifies SSL certificates to be used for encryption.	To specify the HTTPS certificate, select a certificate from the HTTPS Certificate list—for example, new .
	This field is available only after you have created an SSL certificate.	
Enable HTTPS 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.

Table 6: Secure Access Quick Configuration Summary (*continued*)

Field	Function	Your Action
HTTPS-Enabled Interfaces	Allows you to specify interfaces on which you want to enable HTTPS access.	<p>Select and deselect interfaces by clicking the direction arrows:</p> <ul style="list-style-type: none"> ■ To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. ■ To disable HTTPS access on an interface, add the interface to the Logical Interfaces list.
JUNOScript over SSL		
Enable SSL JUNOScript access	Enables secured SSL access to the JUNOScript XML scripting API.	To enable SSL access, select the Enable SSL JUNOScript access check box.
JUNOScript SSL 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 SSL Certificate list—for example, new .

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 13.

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 System Basics Configuration Guide*.

Viewing Current Users

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

Lost Router Connectivity

- | | |
|-----------------|--|
| Problem | After completing initial configuration, I lost connectivity to the routing platform through J-Web. |
| Cause | For J-series routing platforms only, after initial configuration is complete, the routing platform stops functioning as a 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 am unable to access J-Web from my browser. |
|----------------|--|

Solution **Solution 1**—On an M-series or T-series routing platform, 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 3.

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

Chapter 2

J-Web User Interface Overview

- J-Web Overview on page 17
- J-Web Layout on page 18
- Top Pane Elements on page 19
- Main Pane Elements on page 20
- Side Pane Elements on page 21
- Navigating the J-Web Interface on page 22
- Navigating the Quick Configuration Pages on page 22
- Navigating the J-Web Configuration Editor on page 22
- Getting J-Web Help on page 23

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 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. For more information, see “Monitor Tasks” on page 27.
- **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 CLI configuration statements and hierarchy.
 - Edit the configuration in a text file.
 - Upload a configuration file.

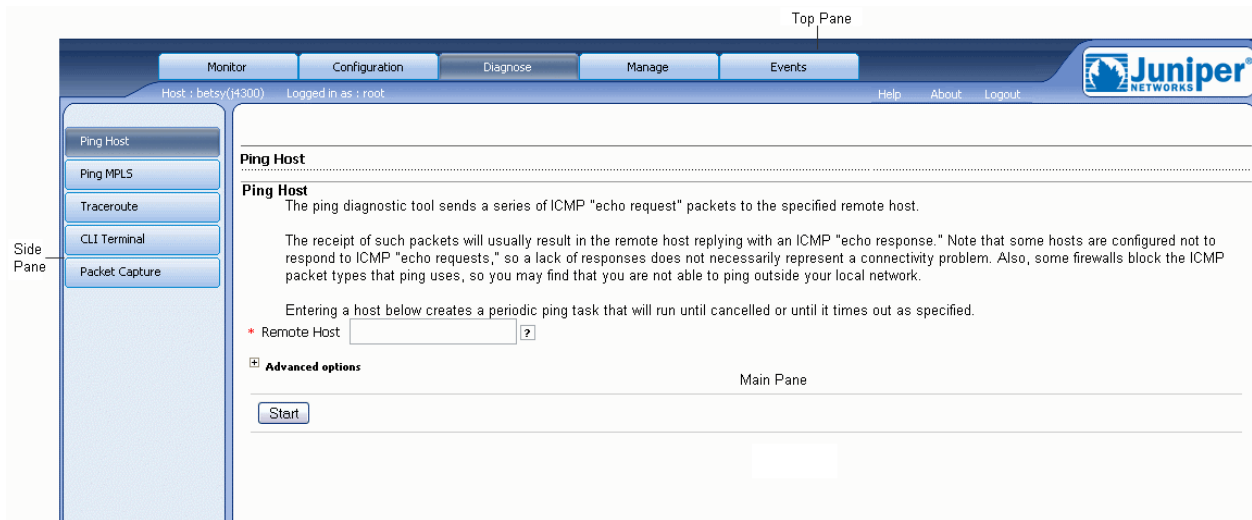
The J-Web interface also allows you to manage configuration history and set a rescue configuration. For more information, see “Configuration Tasks” on page 43.

- Diagnosing—Diagnose routing problems by running the ping or traceroute diagnostic tool. The diagnostic tools also allow you to capture and analyze routing platform control traffic. For more information, see “Diagnose Tasks” on page 73.
- Managing—Manage log, temporary, and core (crash) files and schedule reboots on the routing platforms. On J-series routing platforms, you can also manage software packages and licenses and copy a snapshot of the system software to a backup device. For more information, see “Manage Tasks” on page 85.
- 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. For more information, see “Events Tasks” on page 91.
- Configuring and monitoring alarms—On J-series routing platforms 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. For more information, see “Alarms Tasks (J-series Routing Platforms Only)” on page 99.

J-Web Layout

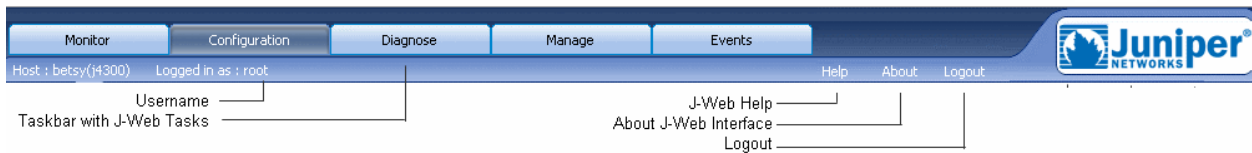
Each page of the J-Web interface is divided into the following panes, as shown in Figure 3 on page 19.

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor, configure, diagnose, and manage the routing platform by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays subtasks of the Monitor, Configuration, Diagnose, or Manage 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 3: J-Web Layout

Top Pane Elements

The top pane comprises the elements shown in Figure 4 on page 19.

Figure 4: 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.
- Help—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.
 - **Monitor**—View information about configuration and hardware on the routing platform.
 - **Configuration**—Configure the routing platform with Quick Configuration or the configuration editor, and view configuration history.
 - **Diagnose**—Troubleshoot network connectivity problems.

- **Manage**—Manage files and licenses, upgrade software, and reboot the routing platform.
- **Events**—View events and set up filters for an event summary.

Main Pane Elements

The main pane comprises the elements shown in Figure 5 on page 20.

Figure 5: Main Pane Elements

Quick Configuration Current task

IPSec Tunnels **Add an IPSec Tunnel**

Tunnel Information

* Local Tunnel Endpoint ? Help Icon

* Remote Tunnel Endpoint ? Help Information

* IKE Secret Key ?

* Verify IKE Secret Key

Private Prefix List ?

Red asterisk (required field)

Add Delete

OK Cancel

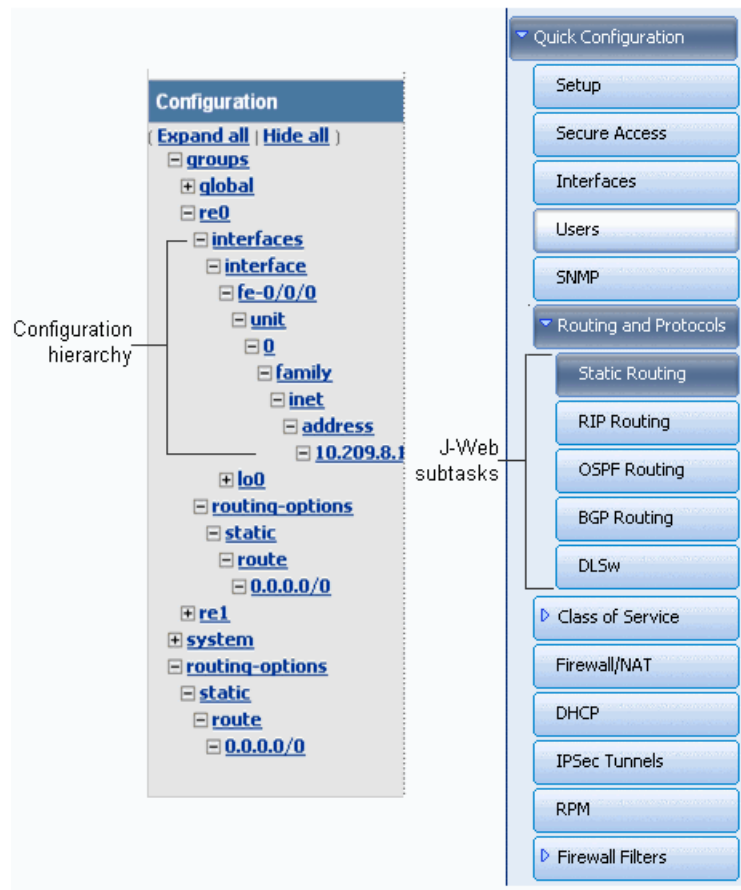
Local Tunnel Endpoint
Externally routable IP address that is the local endpoint of the IPSec tunnel.

- 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 6 on page 21.

Figure 6: 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. Most buttons and links are self-explanatory. But some buttons have different functions on the Quick Configuration and Edit Configuration (J-Web configuration editor) pages. For more information, see “Navigating the Quick Configuration Pages” on page 22 and “Navigating the J-Web Configuration Editor” on page 22.

Navigating the Quick Configuration Pages

Table 7 on page 22 describes the functions of key Quick Configuration buttons. For more information, see “Using Quick Configuration” on page 47

Table 7: J-Web Quick Configuration Buttons

Function	Button
Commit your entries into the configuration, and return to the previous J-Web page.	OK
Clear the entries you have not yet applied to the configuration, and return to the previous J-Web page.	Cancel
Commit your entries into the configuration, and stay on the same J-Web page.	Apply

Navigating the J-Web Configuration Editor

When you select **Edit Configuration** (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 “Edit Configuration Page (J-Web Configuration Editor)” on page 55

After typing or selecting your configuration edits, click a button in the main pane (described in Table 8 on page 23) to move to the previous page after applying or committing the configuration. An updated configuration does not take effect until you commit it.

Table 8: 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 62	Commit

Getting J-Web Help

The J-Web interface provides two ways to display Help for the Monitor, Quick Configuration, Diagnose, Manage, Events, and Alarms tasks. For Help on the View and Edit configuration tasks, see the related documentation provided in the [\[Unresolved xref\]](#).

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 7 on page 24 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 7: CoS Help Page

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

Configuring CoS with Quick Configuration

The Class of Service Quick Configuration pages allow you to configure most of the JUNOS CoS components for the IPv4, IPv6, and MPLS traffic on a routing platform. You can configure forwarding classes for transmitting packets, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a random early detection (RED) algorithm. After defining the CoS components you must assign classifiers to the required physical and logical interfaces.

This section contains the following topics:

- [Defining CoS Components](#)
- [Defining CoS Value Aliases](#)
- [Defining Forwarding Classes](#)
- [Defining Classifiers](#)
- [Defining Rewrite Rules](#)
- [Defining Schedulers](#)
- [Defining Virtual Channel Groups](#)
- [Assigning CoS Components to Interfaces](#)

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

Part 2

J-Web Tasks

- Monitor Tasks on page 27
- Configuration Tasks on page 43
- Diagnose Tasks on page 73
- Manage Tasks on page 85
- Events Tasks on page 91
- Alarms Tasks (J-series Routing Platforms Only) on page 99

Chapter 3

Monitor Tasks

- Monitor Task Overview on page 27
- System on page 28
- Chassis on page 28
- Interfaces on page 29
- Routing on page 29
- Class of Service on page 30
- MPLS on page 31
- Service Sets on page 32
- Firewall on page 33
- IPSec on page 33
- NAT on page 34
- DHCP (J-series Routing Platforms Only) on page 34
- RPM on page 35
- PPPoE (J-series Routing Platforms Only) on page 36
- FEB Redundancy (M120 Routing Platforms Only) on page 36
- Chassis Viewer (M7i, M10i, M20, M120, and M320 Routing Platforms Only) on page 37
- Sample Task—Monitoring Interfaces on page 38
- Sample Task—Monitoring Route Information on page 40

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 77. For more information about the **show** commands, see the JUNOS 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. (See “Sample Task—Monitoring Route Information” on page 40.)

System

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** in the J-Web interface.

Table 9 on page 28 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 9: System Information and 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

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

Table 10 on page 28 shows a summary of the information displayed on the Chassis page and the corresponding CLI **show** commands you can enter at the J-Web CLI terminal.

Table 10: Chassis Information and 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

Table 10: Chassis Information and Corresponding CLI show Commands (*continued*)

Information Displayed	Corresponding CLI Command
Status information about the installed FPCs and PICs.	<code>show chassis fpc</code>
List of all FPCs and PICs installed in the routing platform chassis, including the hardware version level and serial number.	<code>show chassis hardware</code>

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 Interfaces Summary page. (See “Sample Task—Monitoring Interfaces” on page 38.)

Table 11 on page 29 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 11: Interfaces Information and Corresponding CLI show Commands

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

Routing

To view information about routes in a routing table or for information about OSPF, BGP, RIP, or 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 **OK**. (See “Sample Task—Monitoring Route Information” on page 40).

Table 12 on page 30 shows a summary of the information displayed on Routing pages and the corresponding CLI `show` commands you can enter at the J-Web CLI terminal.

Table 12: Routing Information and 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
BGP Information	
Summary about Border Gateway Protocol (BGP).	show bgp summary
BGP peers.	show bgp neighbor
OSPF Information	
Information about Open Shortest Path First (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 routing platforms.	show rip statistics
RIP neighbors.	show rip neighbors
DLSw Information (J-series Routing Platforms only)	
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

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 13 on page 31 shows a summary of the information displayed on Class of Service pages and the corresponding CLI show commands you can enter at the J-Web CLI terminal.

Table 13: Class of Service Information and 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 Differentiated Services 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

MPLS

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

Table 14 on page 31 shows a summary of the information displayed on MPLS pages and the corresponding CLI show commands you can enter at the J-Web CLI terminal.

Table 14: MPLS Information and 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	

Table 14: MPLS Information and Corresponding CLI show Commands *(continued)*

Information Displayed	Corresponding CLI Command
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

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 15 on page 32 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 15: Service Sets Information and 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

Firewall

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

Table 16 on page 33 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 16: Firewall Information and 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 IPSec tunnels and statistics, and IKE security associations for adaptive services interfaces select **Monitor > IPSec** in the J-Web interface.

Table 17 on page 33 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 17: IPSec Information and 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

Table 17: IPSec Information and Corresponding CLI show Commands *(continued)*

Information Displayed	Corresponding CLI Command
(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 > NAT** in the J-Web interface.

Table 18 on page 34 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 18: NAT Information and Corresponding CLI show Command

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

DHCP (J-series Routing Platforms Only)

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 > DHCP** in the J-Web interface.

Table 19 on page 34 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 19: DHCP Information and 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
DHCP server statistics.	show system services dhcp statistics

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 **Monitor > RPM** in the J-Web interface.

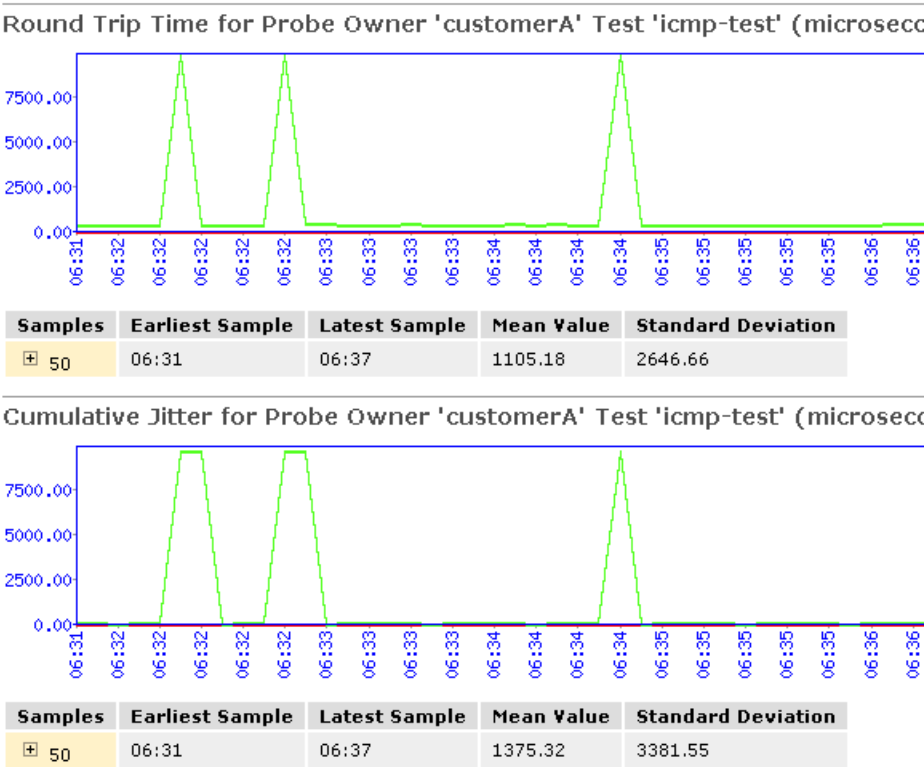
Table 20 on page 35 shows a summary of the information displayed on the RPM page and the corresponding CLI show command you can enter at the J-Web CLI terminal.

Table 20: RPM Information and 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 8 on page 35 shows sample graphs for an RPM test.

Figure 8: Sample RPM Graphs



In Figure 8 on page 35, 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.

PPPoE (J-series Routing Platforms Only)

The PPPoE monitoring information is displayed in multiple parts. To display the session status for PPPoE interfaces, cumulative statistics for all PPPoE interfaces on the 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 21 on page 36 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 21: PPPoE Information and 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

FEB Redundancy (M120 Routing Platforms Only)

On M120 routing platforms, 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 > Chassis > FEB Redundancy** in the J-Web interface.

Table 22 on page 36 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 22: FEB Redundancy Information and Corresponding CLI show Command

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

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

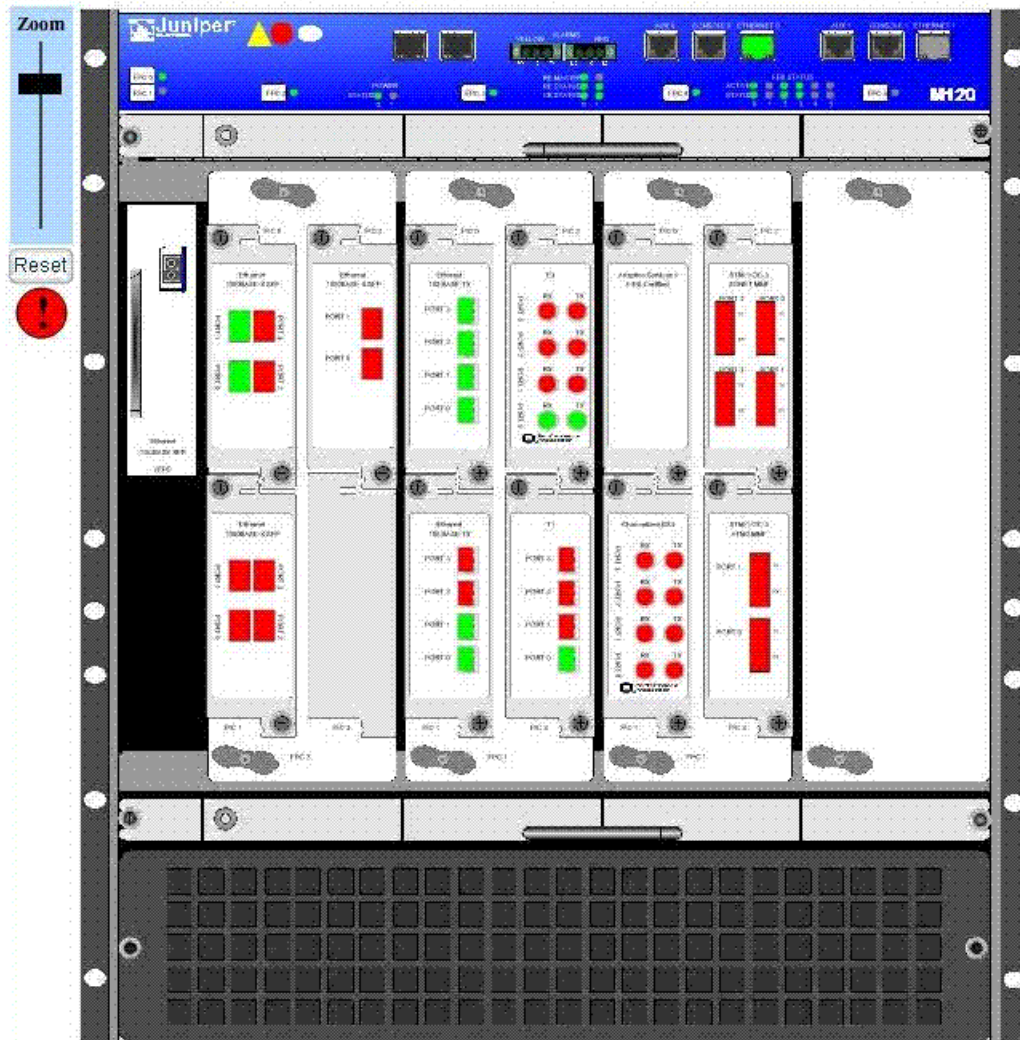
On M7i, M10i, M20, M120, and M320 routing platforms, you can use the chassis viewer feature to view images of the chassis and access information about each component similar to what you can obtain using the **show chassis alarms** and **show chassis hardware** commands.

To access the chassis viewer, click the Chassis Viewer icon 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 9 on page 38 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 9: 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.



Sample Task—Monitoring Interfaces

Figure 10 on page 39 shows the Interfaces Summary 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 10: Monitoring Interfaces Page

Interfaces			
Interface Summary			
Interface Name	Oper State	Admin State	Description
fe-0/0/0	Up	Up	
fe-0/0/0.0			
	inet	Address	10.209.8.129 ⇒ 10.209.0/18
qr-0/0/0	Up	Up	
ip-0/0/0	Up	Up	
ls-0/0/0	Up	Up	
lt-0/0/0	Up	Up	
mt-0/0/0	Up	Up	
pd-0/0/0	Up	Up	
pe-0/0/0	Up	Up	
sp-0/0/0	Up	Up	
sp-0/0/0.16383			
	inet		
fe-0/0/1	Down	Up	
ct1-2/0/0	Down	Up	
ct1-2/0/1	Down	Up	
dsc	Up	Up	
gre	Up	Up	
ipip	Up	Up	
lo0	Up	Up	
lo0.0			
	inet	Address	127.0.0.1
lo0.16385			
		Address	10.0.0.1
		Address	10.0.0.16
	inet	Address	128.0.0.1
		Address	128.0.1.16
lo0.32768			
lsi	Up	Up	
mtun	Up	Up	
pimd	Up	Up	
pime	Up	Up	
pp0	Up	Up	
tap	Up	Up	

You can click any interface to view details about its status. For example, clicking [fe-0/0/0.0](#) displays detailed information about the interface (see Figure 11 on page 40).

Figure 11: Interface fe-0/0/0.0 Monitoring Page**Interfaces****Interface: fe-0/0/0.0**

fe-0/0/0.0				
Encapsulation: ENET2				
Traffic statistics	Packets	PPS	Bytes	BPS
Input	33383642		2282699643	
Output	120607		41023024	
Local traffic statistics	Packets	PPS	Bytes	BPS
Input	33251893		2270424631	
Output	55122		33044087	
Transit traffic statistics	Packets	PPS	Bytes	BPS
Input	131749	0	12275012	14328
Output	65485	0	7978937	0
Family: inet	MTU: 1500	Flags: Is-Primary	Route Table: 0	
Local	Destination	Broadcast	Flags	
10.209.8.129	10.209.0/18	10.209.63.255	Is-Default Is-Preferred Is-Primary	

Sample Task—Monitoring Route Information

Figure 12 on page 41 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 12: 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
<div>⊕ 0.0.0.0/0</div>	*Static/5	Router	2w2d 19:46:24
<div>⊕ 10.10.0.0/16</div>	*Static/5	Router	2w2d 19:46:24
<div>⊕ 10.209.0.0/18</div>	*Direct/0	Interface	2w2d 19:46:24
<div>⊕ 10.209.8.129/32</div>	*Local/0	Local	2w2d 19:46:26
<div>⊕ 172.16.0.0/12</div>	*Static/5	Router	2w2d 19:46:24
<div>⊕ 192.168.0.0/16</div>	*Static/5	Router	2w2d 19:46:24
<div>⊕ 192.168.102.0/23</div>	*Static/5	Router	2w2d 19:46:24
<div>⊕ 207.17.136.0/24</div>	*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

25

OK

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 13 on page 42).

Figure 13: 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
<input type="checkbox"/> 10.209.0.0/18	*Direct/0	Interface	2w2d 22:01:22

Narrow Search

Destination Address

Next Hop Address

Best Route ☐

Exact Route ☐

Number of Routes to Display

Protocol

Receive Protocol

Inactive Routes ☐

Hidden Routes ☐

Chapter 4

Configuration Tasks

- Configuration Task Overview on page 43
- Editing and Committing a JUNOS Configuration on page 45
- J-Web Configuration Tasks on page 46
- Using Quick Configuration on page 47
- Sample Task—Configuring Setup with Quick Configuration on page 49
- Configuring the Router Identification on page 50
- Configuring the Network on page 51
- Configuring the Management Access on page 51
- Sample Task—Configuring Firewall Filters with Quick Configuration on page 51
- View Configuration Text on page 53
- Edit Configuration Page (J-Web Configuration Editor) on page 55
- Editing a Configuration on page 58
- Discarding Parts of a Candidate Configuration on page 61
- Committing a Configuration on page 62
- Accounting Options on page 62
- Edit Configuration Text on page 64
- Upload Configuration File on page 65
- Displaying Configuration History on page 66
- Displaying Users Editing the Configuration on page 68
- Comparing Configuration Files on page 69
- Downloading a Configuration File on page 70
- Loading a Previous Configuration File on page 71
- Using Rescue (J-series Routing Platforms Only) on page 71

Configuration Task Overview

The J-Web user interface provides different methods for configuring your routing platform with the JUNOS software. 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 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 77. For complete information about using the CLI, see the *JUNOS 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.

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 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. (See “Sample Task—Configuring Setup with Quick Configuration” on page 49.)

To better understand the JUNOS configuration process, become familiar with the terms defined in Table 23 on page 44.

Table 23: JUNOS 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 software 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.

Table 23: JUNOS Configuration Terms (*continued*)

Term	Definition
rescue configuration	On J-series routing platforms 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.

Editing and Committing a JUNOS 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 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. (See “Sample Task—Configuring Setup with Quick Configuration” on page 49.)

To better understand the JUNOS configuration process, become familiar with the terms defined in Table 23 on page 44.

Table 24: JUNOS 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.

Table 24: JUNOS Configuration Terms (*continued*)

Term	Definition
configuration hierarchy	Set of hierarchically organized configuration statements that make up the JUNOS software 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 routing platforms 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.

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 25 on page 46 provides a summary of the J-Web configuration tasks.

Table 25: J-Web Configuration Tasks Summary

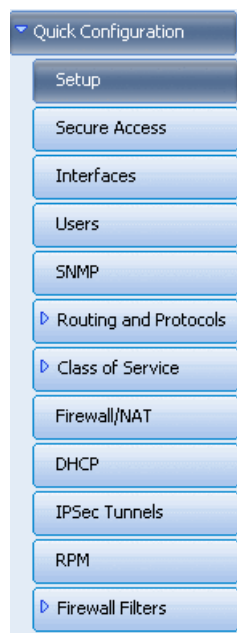
J-Web Configuration Task	Description	More Information
Edit the configuration quickly	Set up, configure, and manage the routing platform quickly and easily without configuring each statement individually.	“Using Quick Configuration” on page 47
Edit the configuration using a clickable interface	Expand 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.	“Edit Configuration Page (J-Web Configuration Editor)” on page 55
Edit the configuration in a text format	Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines in the configuration text.	“Edit Configuration Text” on page 64
Upload a configuration file	Upload a complete configuration.	“Upload Configuration File” on page 65
View the configuration in text format	View the entire configuration on the routing platform in text format.	“View Configuration Text” on page 53
Display configuration history	Display the routing platform configuration history and compare, roll back, or download specific versions of the configuration.	“Displaying Configuration History” on page 66
Display users editing the configuration	Display information about all users logged into a routing platform at the same time.	“Displaying Users Editing the Configuration” on page 68

Table 25: J-Web Configuration Tasks Summary *(continued)*

J-Web Configuration Task	Description	More Information
Set and delete a rescue configuration	On J-series routing platforms, create or delete a rescue configuration.	“Using Rescue (J-series Routing Platforms Only)” on page 71

Using Quick Configuration

To access Quick Configuration, select **Configuration > Quick Configuration**. You select a Quick Configuration task by clicking it in the side pane, or selecting it in the main pane. Quick Configuration pages provide access to the most commonly configured parameters for most supported features. Figure 14 on page 47 shows the Quick Configuration tasks on a J-series routing platform.

Figure 14: J-Web Quick Configuration Tasks

Depending on the complexity of the feature you want to configure, use the Quick Configuration tasks as follows:

- For simple features—Quick Configuration allows you to perform basic configurations easily. It simplifies configuration by combining a few actions in one, so that you are not required to configure each statement individually. For example, the Set Up Quick Configuration page allows you to easily perform all configuration required for setting up basic connectivity from one single page. (See “Sample Task—Configuring Setup with Quick Configuration” on page 49.)
- For complex features—Quick Configuration allows you to view existing configurations at a glance and edit and manage them easily. Because it provides a complete view of configurations on a single page, Quick Configuration is a very useful tool for planning and managing complex features. For example, the

Stateless Firewall Filter Quick Configuration page displays multiple filters and terms as rows that you can reorder by simply clicking on up or down arrows. Match conditions and actions are displayed as intuitive icons. (See “Sample Task—Configuring Firewall Filters with Quick Configuration” on page 51.)

Table 26 on page 48 lists key Quick Configuration tasks and their functions.

Table 26: Quick Configuration Tasks Summary

Quick Configuration Task	Function
Setup	Define network identification, default gateway, name and time servers, root user authentication, and basic local network access to the system.
Secure Access	Configure certificates, secure access methods, and interfaces to enable HTTP and HTTPS Web management.
Interfaces	List all interfaces installed on the system, and configure logical interfaces and common interface parameters.
Users	Define users allowed to access the routing platform, and configure authentication servers. Pick an authorization level for each user.
SNMP	Configure Simple Network Management Protocol (SNMP) access to a device. Define SNMP communities. Specify which SNMP traps are generated and the recipients of those traps.
Routing and Protocols (J-series routing platforms only)	Define default and static routes, and the basic routing configuration for the following routing protocols: <ul style="list-style-type: none"> ■ Open Shortest Path First (OSPF) ■ Routing Information Protocol (RIP) ■ Border Gateway Protocol (BGP) ■ Data Link Switching (DLSw)
Class of Service	Define class-of-service (CoS) components to provide differentiated services when best-effort traffic delivery is not sufficient.
FEB Redundancy (M120 routing platform only)	Configure Forwarding Engine Board (FEB) redundancy groups to provide high availability for FEBs. FEBs provide route lookup and forwarding functions from Flexible PIC Concentrators (FPCs) and compact FPCs.
Firewall/NAT (J-series routing platforms only)	Apply a stateful firewall filter to WAN interfaces. Choose the applications that are allowed through the firewall from the WAN. Enable Network Address Translation.
DHCP (J-series routing platforms only)	Provide Dynamic Host Configuration Protocol (DHCP) service to specified LAN networks or hosts. Specify DHCP address ranges.
IPSec Tunnels (J-series routing platforms only)	Create IP Security (IPSec) tunnels to private networks.
RPM	Define performance probes and thresholds for real-time performance monitoring (RPM) verification and network performance.
Firewall Filters	Configure input and output firewall filters—also known as access control lists (ACLs). Apply firewall filters to specific interfaces.

Table 27 on page 49 describes the functions of the buttons that appear on J-Web Quick Configuration pages.

Table 27: J-Web Quick Configuration Buttons

Button	Function
Add	Adds statements or identifiers to the configuration.
Delete	Deletes statements or identifiers from the configuration.
OK	Commits your entries into the configuration, and returns you to the previous Web page.
Cancel	Clears the entries you have not yet applied to the configuration, and returns you to the previous J-Web page.
Apply	Commits your entries into the configuration, and stays on the same J-Web page.

Sample Task—Configuring Setup with Quick Configuration

Figure 15 on page 50 shows the Set Up Quick Configuration page. This page allows you to manage and configure basic routing platform setup easily from one location. You name the routing platform, set the root password, assign network addresses and servers. Set the time, and determine your management access by selecting or typing these values.

Figure 15: Set Up Quick Configuration Page

Quick Configuration	
Set Up	
Identification	Time
* Host Name <input type="text" value="carol"/> ? Domain Name <input type="text" value="lab.example.net"/> ? * Root Password <input type="password" value="....."/> ? * Verify Root Password <input type="password" value="....."/>	Time Zone <input type="text" value="America/Los_Angeles"/> ? NTP Servers <input type="text"/> ? <input type="button" value="Add"/> <input type="button" value="Delete"/> Current System Time <input type="text" value="01/20/2009 06:18"/> ? <input type="button" value="Set time now via NTP"/> ? <input type="button" value="Set time now manually"/> ?
Network	Management Access
DNS Name Servers <input type="text" value="10.209.194.131"/> ? <input type="text" value="10.209.194.133"/> ? <input type="text" value="172.17.28.101"/> ? <input type="button" value="Add"/> <input type="button" value="Delete"/> Domain Search <input type="text" value="spglab.juniper.net"/> ? <input type="text" value="apglab.juniper.net"/> ? <input type="text" value="lab.example.net"/> ? <input type="button" value="Add"/> <input type="button" value="Delete"/> Default Gateway <input type="text" value="123.0.1.2"/> Loopback Address <input type="text" value="192.168.8.1/32"/> ? fe-0/0/0.0 Address <input type="text" value="192.168.69.205/21"/>	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 <input checked="" type="checkbox"/> Allow JUNOScript over Clear-Text Access <input type="checkbox"/> The following access method is considered secure as any information sent over it will be encrypted before transmission. Allow SSH Access <input checked="" type="checkbox"/> In order to enable HTTPS or JUNOScript over SSL, you will need to visit the SSL configuration page to configure certificates and associations.
<input type="button" value="Apply"/>	

For more information about setting up your system, see “Configuring Basic Settings” on page 6 and the *JUNOS Software Installation and Upgrade Guide*.

Configuring the Router Identification

To define a hostname, domain name, password, time zone, and system time of the routing platform:

1. Make sure that the tasks described in the Before you Begin section of “Configuring Basic Settings” on page 6 were performed.
2. Navigate to the Set Up Quick Configuration page by selecting **Configuration > Quick Configuration > Set Up** (see Figure 15 on page 50).
3. Next to Host Name, type **carol** to define the name of the routing platform.
4. Next to Domain Name, type **lab.example.net** to define the network that the machine belongs to.
5. Next to Root Password, type a plain-text password to set the root password for logging in to the routing platform.
6. Next to Verify Root Password, retype the password to verify that you typed the root password correctly.

7. From the Time Zone list, select **America/Los_Angeles** to specify the time zone that the routing platform is located in.
8. Click **Set Time via NTP** to synchronize the system time with the NTP server. The routing platform sends a request to the NTP server and synchronizes the system time.

Configuring the Network

To define the DNS server, default gateway, loopback address, and management address of the routing platform:

1. Under DNS Name Servers, type **172.17.28.101** and click **Add** to specify the IP address of the DNS server that the routing platform can use to resolve hostnames into addresses.
2. Next to Domain Search, type **lab. example.net** to include the domain name in a DNS search.
3. Next to Default Gateway, type **123.0.1.2** to define a default gateway through which to direct packets addressed to networks not explicitly listed in the routing table.
4. Next to Loopback Address, type **192.168.8.1/32** to define a reserved IP address that will always be available on the routing platform.
5. Next to fxp0 Address, type **192.168.69.205/21** to define the IP address and prefix length of the management interface. The management interface is used for accessing the routing platform.

Configuring the Management Access

To define the management access settings for the routing platform:

1. Next to Allow Telnet Access, select the check box to allow remote Telnet access to the routing platform.
2. Next to Allow SSH Access, selected the check box to allow remote SSH access to the routing platform.
3. Click **Apply** to apply the configuration.

Sample Task—Configuring Firewall Filters with Quick Configuration

Figure 16 on page 53 shows the Firewall Filter Quick Configuration page. This page allows you to view multiple filters and terms on a single page and reorder them by simply clicking up or down arrows. Match conditions and actions are displayed as intuitive icons. You can also search for a filter by name and display a specified number of filters on the page.

In this example, the Firewall Filters Quick Configuration page shows two filters—**filter1** and **filter2**. The expanded **filter2** displays three terms. Each term consists of two components—match conditions and actions. The match conditions define the values

or fields that the packet must contain to be considered a match. If a packet is a match, the corresponding action is taken. By default, a packet that does not match a firewall filter is discarded. The icons displayed across each term indicate the associated match condition and action:

- **term 1**—Accepts any packet with 3.3.0.0/24 as a source or destination address.
- **term 2**—Matches any packet with an **ldp** source or destination port and sets a low PLP bit on the packet.
- **term 3**—Discards any packet with a destination address 10.0.0.0/24.

The order of the terms and filters is important. The routing platform compares a route against the match conditions of each term in a routing policy, starting with the first and moving through the terms in the order in which they are defined, until a match is made. If none of the terms in the policy match the route, the routing platform compares the route against the next policy, and so on, until either an action is taken or the default policy is evaluated. The Firewall Filter Quick Configuration page allows you to reorder terms and filters by clicking up or down arrows and thus simplifies management of complex filters.

Figure 16: Firewall Filter Quick Configuration Page

Quick Configuration

Firewall Filters

Firewall Filters

IPv4 Filter Summary Showing filters 1 to 2 of 2 total. (Page 1 of 1)

Filter Name									
↓ X	filter 1								
↑ X	filter 2								
	Term Name	Action	Protocol	Source Address	Source Port	Destination Address	Destination Port	Address	Port
↓ X	term1	✓	*	3.3.0.0/24	*	3.3.0.0/24	*	*	*
↑ ↓ X	term2	PLP	*	*	*	*	*	*	ldp
↑ X	term3	✗	*	*	*	10.0.0.0/24	*	*	*

Legend

✓ Accept Packet ?

✗ Reject Packet ?

✗ Discard Packet ?

↓ Evaluate Next Term ?

→ Routing Instance ?

Log Packet ?

Syslog Packet ?

Count Packet ?

PLP Set Packet Loss Priority ?

Logical Router ?

Load Balance Packet ?

RL Rate Limit (Police) Packet ?

Any firewall term match conditions that are colored red are considered negated. If a packet matches a negated condition, it is immediately considered not to match the term statement, and the next term in the filter is evaluated. Note that the order of the terms within a firewall filter is significant. Packets are tested against each term in the order in which they are listed in the configuration.

Add New IPv4 Filter

Search

Name

After Final IPv4 Filter ?

After IPv4 Filter ?

Before IPv4 Filter ?

filter 1

filter 1

Add

IPv4 Filter Name

IPv4 Term Name

Number of Items to Display

25

OK

View Configuration Text

To view the entire configuration in text format, select **Configuration > View and Edit > View Configuration Text**. The main pane displays the configuration in text format (see Figure 17 on page 54). The displayed configuration is the same as the configuration displayed when you enter the JUNOS CLI command `show configuration`.

Figure 17: View Configuration Text Page**View and Edit****View Configuration Text**

The current configuration running on the device

```
## Last commit: 2008-12-23 09:28:24 UTC by regress
version "9.4I0 [builder]";
groups {
  global {
    system {
      host-name betsy;
      domain-name juniper.net;
      domain-search [ englab.juniper.net apglab.juniper.net spglab.juniper.net juniper.net jnpr.net ];
      backup-router 10.209.63.254 destination 0.0.0.0/0;
      root-authentication {
        encrypted-password Nxvw9kdviPB.s;
      }
      name-server {
        10.209.194.131;
        10.209.194.133;
      }
      login {
        user regress {
          uid 928;
          class superuser;
          shell csh;
          authentication {
            encrypted-password "$1$kPU..$w.4FCRA&anJ8U4Yq6sbj7.";
          }
        }
      }
      services {
        ftp;
        rlogin;
        rsh;
        ssh;
        telnet;
      }
    }
  }
  routing-options {
    static {
      route 172.16.0.0/12 {
        next-hop 10.209.63.254;
        retain;
        no-readvertise;
      }
      route 192.168.0.0/16 {
        next-hop 10.209.63.254;
        retain;
        no-readvertise;
      }
      route 10.10.0.0/16 {
        next-hop 10.209.63.254;
        retain;
        no-readvertise;
      }
    }
  }
}
```

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 17 on page 54 shows that user **regress** committed the last configuration on 23 December 2008, and the software version running on the routing platform is JUNOS Release 9.4.

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.

Edit Configuration Page (J-Web Configuration Editor)

Using View and Edit, you can configure all properties of the JUNOS software, 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 **Configuration > View and Edit > Edit Configuration**. This page allows you to configure all routing platform services that you can configure from the JUNOS 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 28 on page 55 lists key J-Web configuration editor tasks and their functions.

Table 28: 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 <i>JUNOS System Basics Configuration Guide</i> .
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 <i>JUNOS Network Management Configuration Guide</i> .

Table 28: J-Web Configuration Editor Tasks Summary (*continued*)

J-Web Configuration Editor Task	Function
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 <i>JUNOS Services Interfaces Configuration Guide</i> .
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 <i>JUNOS System Basics Configuration Guide</i> .
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 <i>JUNOS Class of Service Configuration Guide</i> .
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 software operational mode commands, or execute JUNOS event scripts (op scripts). For more information, see the <i>JUNOS Configuration and Diagnostic Automation Guide</i> .
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 <i>JUNOS Policy Framework Configuration Guide</i> .
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 <i>JUNOS Policy Framework Configuration Guide</i>.</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 <i>JUNOS Network Interfaces Configuration Guide</i> .
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 <i>JUNOS VPNs Configuration Guide</i> .

Table 28: 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 <i>JUNOS Routing Protocols Configuration Guide</i> and the <i>JUNOS MPLS Applications Configuration Guide</i> .
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 <i>JUNOS Routing Protocols Configuration Guide</i> .
Routing options	<p>Configure protocol-independent routing options that affect system-wide 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 system-wide tracing (debugging) to track standard and unusual routing operations and record this information in a log file. <p>For more information, see the <i>JUNOS Routing Protocols Configuration Guide</i></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 <i>JUNOS System Basics Configuration Guide</i> .
Services	Configure application settings for services interfaces, such as dynamic flow capture parameters, the Intrusion Detection System (IDS), IPSec VPN service, RPM, stateful firewalls, and Network Address Translation (NAT). For more information, see the <i>JUNOS Services Interfaces Configuration Guide</i> .
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 <i>JUNOS Network Management Configuration Guide</i> .
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 <i>JUNOS System Basics Configuration Guide</i> .

Editing a Configuration

To edit the configuration on a series of pages of clickable options that step you through the hierarchy, select **Configuration > View and Edit > Edit Configuration**. 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 18 on page 59).

Figure 18: Edit Configuration Page

Configuration

[Expand all](#) | [Hide all](#)

+

[groups](#)

+

[system](#)

+

[routing-options](#)

Configuration

Refresh

Commit...

Discard...

Access

[Configure](#)

Accounting options

[Configure](#)

Applications

[Configure](#)

Chassis

[Configure](#)

Class of service

[Configure](#)

Event options

[Configure](#)

Firewall

[Configure](#)

Forwarding options

[Configure](#)

Interfaces

[Configure](#)

Policy options

[Configure](#)

Protocols

[Configure](#)

Routing instances

[Configure](#)

Routing options

[Edit](#) [Delete](#)

Security

[Configure](#)

Services

[Configure](#)

Snmp

[Configure](#)

System

[Edit](#) [Delete](#)

Access profile

Access profile name

?

Advanced

Apply groups

[Add new entry](#)

Value	Actions
re0	Edit Delete
re1	Edit Delete
global	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.

*

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 29 on page 60 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 29: 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 30 on page 60 describes the meaning of these icons.

Table 30: 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.

Table 30: J-Web Edit Configuration Icons (*continued*)

Icon	Meaning
*	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 CLI User Guide*.

After typing or selecting your configuration edits, click a button in the main pane (described in Table 31 on page 61) 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 31: 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 62
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 61.

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 (also known as a radio 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.

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 68. For more information about editing an exclusive candidate configuration, see the *JUNOS 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**.

Accounting Options

Figure 19 on page 63 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 19: 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]

Edit Configuration Text

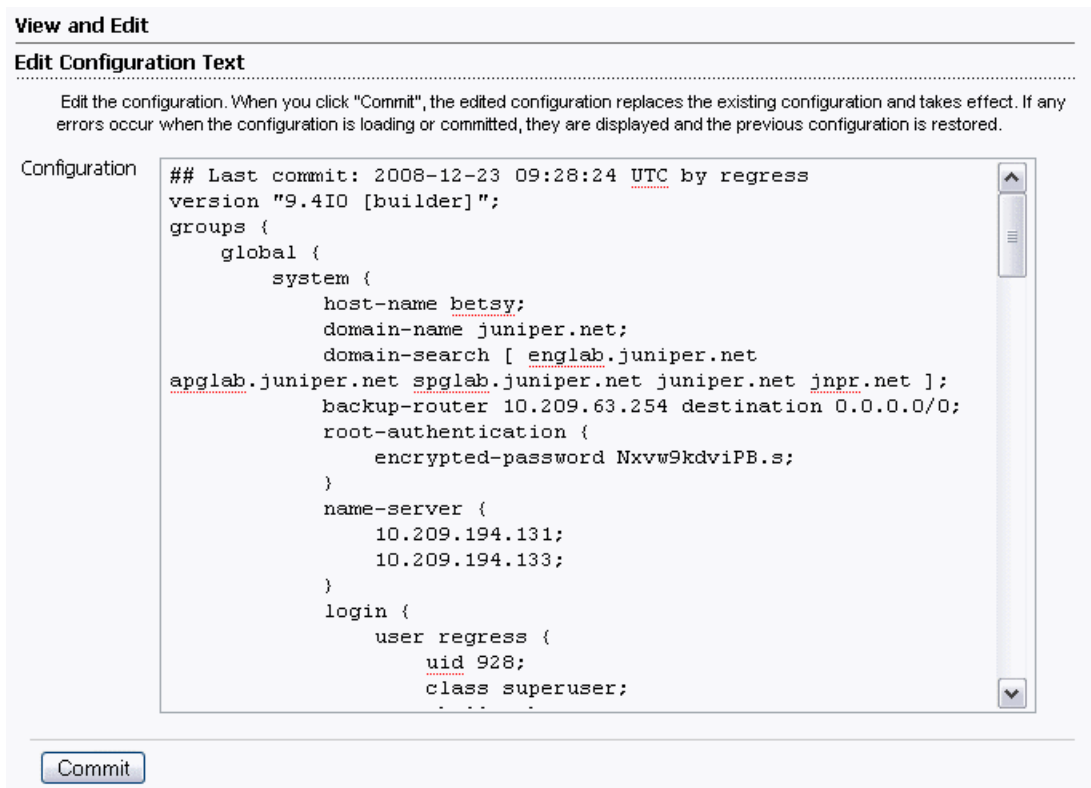
Using View and Edit, you can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties.

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 **Configuration > View and Edit > Edit Configuration Text**. The main pane displays the configuration in a text editor (see Figure 20 on page 64).

Figure 20: Edit Configuration Text Page



For more information about the format of an ASCII configuration file, see “View Configuration Text” on page 53.



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 CLI User Guide*.

Upload Configuration File

To upload a configuration file from your local system:

1. Select **Configuration > View and Edit > Upload Configuration File**.

The main pane displays the File to Upload box (see Figure 21 on page 66).

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 21: J-Web Upload Configuration File Page

View and Edit

Upload Configuration File

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 loading or committing, they are displayed and the previous configuration is restored.

* File to Upload ?

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 **Configuration > History**. The main pane displays Database Information and Configuration History (see Figure 22 on page 67).

Table 32 on page 67 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 22: 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".

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 32: 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 32: 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 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 “Edit Configuration Text” on page 64. ■ 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 65. ■ Modified via quick-configuration—Configuration was modified with the J-Web Quick Configuration tool specified by <i>quick-configuration</i>. For more information, see “Using Quick Configuration” on page 47. ■ 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 71.
Action	<p>Action to perform with the configuration file. The action can be Download or Rollback. For more information, see “Downloading a Configuration File” on page 70 and “Loading a Previous Configuration File” on page 71.</p>

For more information about saved versions of configuration files, see “Editing and Committing a JUNOS Configuration” on page 45.

Displaying Users Editing the Configuration

To display a list of users editing the routing platform configuration, select **Configuration > History**. The list is displayed as Database Information in the main pane (see Figure 23 on page 69). Table 33 on page 69 summarizes the Database Information display.

Figure 23: 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 33: 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.

Comparing Configuration Files

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

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 22 on page 67). Table 32 on page 67 summarizes the Configuration History display.

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

The main pane displays the differences between the two configuration files at each hierarchy level as follows (see Figure 24 on page 70):

- 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 24: J-Web Configuration File Comparison Results**History****Compare Rollback 5 Configuration to Rollback 2 Configuration**

Rollback 5 Configuration		Rollback 2 Configuration	
[edit]		[edit]	
version 9.1B2.8;		version "9.4I0 [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;	
		}	
		}	

Downloading a Configuration File

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

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 22 on page 67). Table 32 on page 67 summarizes the Configuration History display.

2. In the Action column, click **Download** for the version of the configuration you want to download.

3. 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.

Loading a Previous Configuration File

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

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 22 on page 67). Table 32 on page 67 summarizes the Configuration History display.

2. 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.

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 **Configuration > Rescue**. On the Rescue page (see Figure 25 on page 72), 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 25: 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](#)

Chapter 5

Diagnose Tasks

- Using Ping Host on page 73
- Using Ping MPLS on page 74
- Using Ping ATM (M-series, MX-series, and T-series Routing Platforms only) on page 75
- Using Traceroute on page 76
- Using Packet Capture on page 76
- Using the CLI Terminal on page 77
- CLI Terminal Requirements on page 78
- Starting the CLI Terminal on page 79
- Sample Task—Ping Host on page 80

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 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 in the Ping Host page creates a periodic ping task that runs until cancelled 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 77. For more information about the **ping** command, see the *JUNOS 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™ Software 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™ Software 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 74 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 77.

Table 34: Ping MPLS Tasks Summary and 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™ Software pings a particular LSP using the configured LSP name.	When an RSVP-signaled LSP has several paths, the JUNOS™ Software 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™ Software pings a particular LSP using the forwarding equivalence class (FEC) prefix and length.	When an LDP-signaled LSP has several gateways, the JUNOS™ Software sends the ping requests through the first gateway. Ping requests sent to LDP-signaled LSPs use only the master routing instance.

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

Ping MPLS Task	Corresponding CLI Command	Function	Additional Information
Ping LSP to Layer 3 VPN prefix	ping mpls l3vpn	Checks the operability of the connections related to a Layer 3 VPN. The JUNOS™ Software 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™ Software does not test the connection between a PE router and a customer edge (CE) router.
Locate LSP using interface name	ping mpls l2vpn interface	Checks the operability of the connections related to a Layer 2 VPN. The JUNOS™ Software directs outgoing request probes out the specified interface.	For information about interface names, see the <i>JUNOS Interfaces Command Reference</i> .
Instance to which this connection belongs	ping mpls l2vpn instance	Checks the operability of the connections related to a Layer 2 VPN. The JUNOS™ Software pings on a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier, to test the integrity of the Layer 2 VPN circuit (specified by the identifiers) between the inbound and outbound PE routers.	
Locate LSP from interface name	ping mpls l2circuit interface	Checks the operability of the Layer 2 circuit connections. The JUNOS™ Software directs outgoing request probes out the specified interface.	
Locate LSP from virtual circuit information	ping mpls l2circuit virtual-circuit	Checks the operability of the Layer 2 circuit connections. The JUNOS™ Software 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™ Software 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 routing platforms, 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 77. For more information about the **ping atm** command, see the *JUNOS 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 77. For more information about the **traceroute** command, see the *JUNOS 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 77. For more information about the **monitor traffic** command, see the *JUNOS 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*.

Using the CLI Terminal

The JUNOS 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 command line interface (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 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 CLI, see the *JUNOS CLI User Guide*. For information about configuring and monitoring JUNOS features with the CLI, see the JUNOS manuals in [\[Unresolved xref\]](#).

Figure 26 on page 78 shows the CLI terminal displaying all the options that you can configure in CLI configuration mode.

Figure 26: 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#
```

CLI Terminal Requirements

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

- SSH access—Enable Secure shell (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 6.
- 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 Web site <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 78.
2. In the J-Web interface, select **Diagnose > 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 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 27 on page 80).

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 **Diagnose > CLI Terminal** again, retype your JUNOS password to access the CLI.

Figure 27: 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% █

```

Sample Task—Ping Host

Figure 28 on page 81 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 reach 10.10.2.2 and do not reach 10.10.10.10.

To ping the host:

1. Select **Diagnose > Ping Host** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 28 on page 81).
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 28: Ping Host Diagnose 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

10.2.2.2

?

Advanced options

Don't Resolve Addresses

☐

?

Interface

any

▼

?

Count

10

▼

?

Don't Fragment

☐

?

Record Route

☐

?

Type-of-Service

0

▼

?

Routing Instance

default

▼

?

Interval

1

▼

?

Packet Size

56

?

Source Address

?

Time-to-Live

32

▼

?

Bypass Routing

☐

?

Start

Figure 29 on page 82 displays the results of a successful ping in the main pane, and Table 35 on page 82 provides a summary of the ping host results and output.

Figure 29: Successful Ping Host Results Page

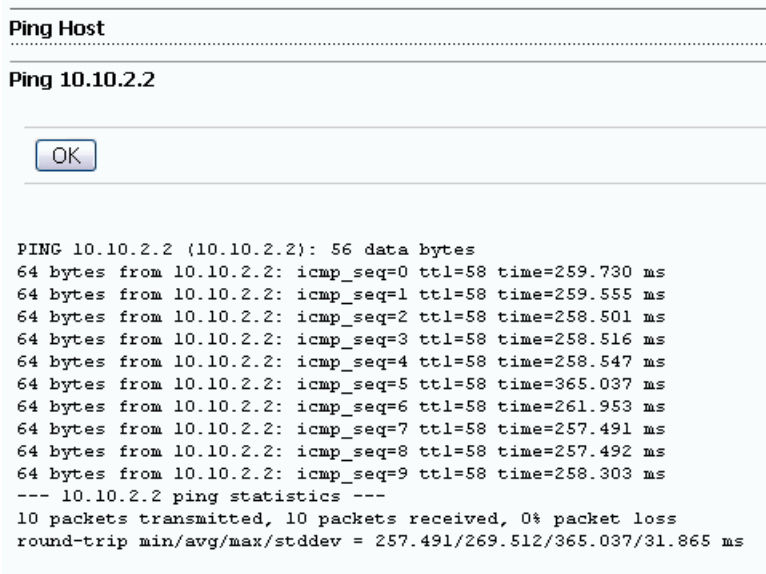


Table 35: J-Web Ping Host Results and Output Summary

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=56	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.
257.492/269.512/365.037/31.865 ms	<ul style="list-style-type: none"> 257.492—Minimum round-trip time 269.51—Average round-trip time 365.03—Maximum round-trip time 31.865—Standard deviation of the round-trip times ms—milliseconds

Figure 30 on page 83 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 30: 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
```


Chapter 6

Manage Tasks

- Using Files on page 85
- Using Software (J-series Routing Platforms Only) on page 86
- Using Licenses (J-series Routing Platform Only) on page 87
- Using Reboot on page 88
- Using Snapshot (J-series Routing Platforms Only) on page 89
- Sample Task—Manage Snapshots on page 90

Using Files

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

Table 36 on page 85 lists the different tasks that you can perform from the Manage > Files page.

Table 36: 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 <code>/cf/var/log</code>—Any files that are not currently being written to are deleted.■ Deletes temporary files in <code>/cf/var/tmp</code>—Any files that have not been accessed within two days are deleted.■ Deletes all crash files in <code>/cf/var/crash</code>—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 <code>request system storage cleanup</code> command at the J-Web CLI terminal. For more information, see “Using the CLI Terminal” on page 77. For more information about the <code>request system storage cleanup</code> command, see the <i>JUNOS System Basics and Services Command Reference</i>.</p>

Table 36: Manage Files Tasks Summary (*continued*)

Manage Files Task	Functions
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 <code>/cf/var/log</code> directory on the router. ■ Temporary Files—Lists the temporary files located in the <code>/cf/var/tmp</code> directory on the router. ■ Old JUNOS Software—Lists the existing JUNOS software packages in the <code>/cf/var/sw</code> directory on the router. ■ Crash (Core) Files—Lists the core files located in the <code>/cf/var/crash</code> 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>

Using Software (J-series Routing Platforms Only)

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

Typically, you upgrade the JUNOS software 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 **Manage > 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 90.

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 System Basics Configuration Guide*.

Table 37 on page 87 lists the different tasks that you can perform from the Manage > Software pages.

Table 37: 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 box is checked, the router is automatically rebooted when the upgrade is complete. Select the check box if you want the router to reboot automatically when the upgrade is complete. <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 box is checked, the router is automatically rebooted when the upgrade is complete. <p>Click Fetch and Install Package to begin.</p>
Downgrade	<p>Downgrade the JUNOS software on the routing platform.</p> <p>When you downgrade the software to a previous version, the software version that is saved in <code>junos.old</code> is the version of JUNOS 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 Manage > 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 software 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 Manage > Licenses page, you can perform the following tasks:

- Add licenses—Add license keys for the following features:
 - Data link switching (DLSw) support
 - J-Flow 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 77. For more information about the commands, see the *JUNOS System Basics and Services Command Reference*.

- `show system license`—Display license information.
- `request system license add`—Add licenses on J-series routing platforms.

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

Using Reboot

The Manage > Reboot page allows you to reboot the routing platform at a specified time. Using the Manage > 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 77. For more information about the `request system reboot` command, see the *JUNOS System Basics and Services Command Reference*.

Using Snapshot (J-series Routing Platforms Only)

The Manage > 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 alternate 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 alternate 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 software 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 31 on page 90 shows a Manage > 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 **Diagnose > Snapshot** from the task bar.
2. Next to Advanced options, click the expand icon (see Figure 31 on page 90).
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 31: 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 ?

Factory ☐ ?

Partition ☐ ?

☐ **Advanced options**

As Primary Media ☒ ?

Data Size ?

Swap Size ?

Config Size ?

Root Size ?

Chapter 7

Events Tasks

- Using View Events on page 91
- Viewing Events on page 92
- Understanding Severity Levels on page 92
- Using Filters on page 93
- Using Regular Expressions on page 95
- Sample Task—Filtering and Viewing Events on page 96
- Troubleshooting Events on page 97

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 32 on page 92 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 select the number of events to be displayed on the screen at a time. You can also 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.

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 77.

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

Figure 32: J-Web View Events Page

View Events

Filters

System Log File	messages ?	Process	?
Event ID	?	Start Time	02/23/2007 17:34 ?
Text in Event Description	?	End Time	02/23/2007 18:34 ?
Number of Events to Display	25		
<input type="button" value="OK"/>			

Event Summary

Showing events 1 to 25 of 599

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

	Unknown	Debug/Info/Notice	Warning	Error	Critical	Alert	Emergency
Time	Process	Event ID	Event Description				
2007-02-23 18:32:01 PST	mgd[4172]	UI_LOGOUT_EVENT ?	User 'regress' logout				
2007-02-23 18:32:01 PST	mgd[4172]	UI_CHILD_STATUS ?	Cleanup child '/sbin/shutdown', PID 4174, status 0				
2007-02-23 18:32:01 PST	mgd[4172]	UI_CHILD_START ?	Starting child '/sbin/shutdown'				
2007-02-23 18:32:01 PST	mgd[4172]	UI_JUNOSCRIP_CMD ?	User 'regress' used JUNOScript client to run command 'get-reboot-information'				
2007-02-23 18:32:01 PST	mgd[4172]	UI_LOGIN_EVENT ?	User 'regress' login, class 'j-superuser' [4172]				
2007-02-23 18:32:01 PST	mgd[4172]	UI_AUTH_EVENT ?	Authenticated user 'regress' at permission level 'j-superuser'				
2007-02-23 18:32:01 PST	mgd[4172]	UI_JUNOSCRIP_CMD ?	User '(unauthenticated user)' used JUNOScript client to run command 'request-authentication user=regress'				
2007-02-23 18:32:00 PST	mgd[4169]	UI_LOGOUT_EVENT ?	User 'regress' logout				
2007-02-23 18:32:00 PST	mgd[4169]	UI_JUNOSCRIP_CMD ?	User 'regress' used JUNOScript client to run command 'request-web-management-update session-id=e0bf98a1b7450bce2c086b9e8338622a'				

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 System Log Messages Reference*.

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 38 on page 93 lists the system log severity levels, the corresponding colors and a description of what the severity level indicates.

Table 38: 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 39 on page 94 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 **OK** to display the filtered events.

Table 39: 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 <i>JUNOS System Log Messages Reference</i>.</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 .
Text in Event 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 95.</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 <i>JUNOS Software Installation and Upgrade Guide</i>.</p>	<p>To specify events generated by a process, type the name of the process.</p> <p>For example, type mgd to list all messages generated by the management process.</p>

Table 39: Summary of Event Filters (*continued*)

Event Filter	Function	Your Action
Start Time	Specifies the time period in which the events you want displayed are generated.	To specify the time period:
End Time	<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. End Time shows the current time and Start Time shows the time one hour before end time.</p>	<ul style="list-style-type: none"> ■ Click the button next to Start Time and select the year, month, date, and time—for example, 02/10/2006 11:32. ■ Click the button next to End Time and select the year, month, date, and time—for example, 02/10/2006 3:32. <p>To select the current time as the start time, select Local Time.</p>

Using Regular Expressions

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

Table 40 on page 95 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 40: 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, <code>.in</code> 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, <code>tre*</code> 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, <code>tre+</code> 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, <code>colou?r</code> matches messages with <i>or color</i> or <i>colour</i>.</p>

Table 40: Common Regular Expression Operators and the Terms They Match (*continued*)

Regular Expression Operator	Matching Terms
(pipe)	One of the terms that appear on either side of the pipe operator. For example, <code>gre ay</code> matches messages with either <i>grey</i> or <i>gray</i> .
! (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.
^ (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 33 on page 97 shows the View Events page displaying filtered events. In this example, you are typing `UI_CHILD_EXITED` in the Event ID box and clicking **OK**. 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 33: J-Web View Events Page

View Events

Filters

System Log File: ?

Event ID: ?

Text in Event Description: ?

Number of Events to Display: ?

Process: ?

Start Time: ?

End Time: ?

Event Summary

Showing events 1 to 2 of 2

Time	Process	Event ID	Event Description
2007-02-23 18:22:35 PST	mgd[21954]	UI_CHILD_EXITED ?	Child exited: PID 21968, status 4, command '/sbin/disklabel'
2007-02-23 18:22:35 PST	mgd[21954]	UI_CHILD_EXITED ?	Child exited: PID 21967, status 4, command

Help: Child process of mgd exited
Description: The management process (mgd) created a child process to execute the indicated command for it. The child process exited unexpectedly with the indicated status code.
Type: Error: An error occurred
Severity: notice

Troubleshooting Events

Problem My View Events page does not display any events. (See Figure 34 on page 97.)

Figure 34: View Events Page Displaying Error

View Events

Filters

System Log File: ?

Event ID: ?

Text in Event Description: ?

Number of Events to Display: ?

Process: ?

Start Time: ?

End 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 on the configuration options, see the *JUNOS System Basics Configuration Guide* (system level) or the *JUNOS 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 35 on page 98.)

Figure 35: 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 8

Alarms Tasks (J-series Routing Platforms Only)

- Using Alarms on page 99
- Active Alarms Information on page 99
- Alarm Severity on page 100
- Displaying Alarm Descriptions on page 100
- Sample Task—Viewing and Filtering Alarms on page 100

Using Alarms

On J-series routing platforms only, 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 77. For more information about the commands, see the *JUNOS System Basics and Services Command Reference*.

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 component, 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 100). 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 36 on page 101 shows the View Alarms page displaying one system alarms that is currently active. The yellow color indicates that the alarms is noncritical. You can also see the time at which the system received the alarm. You can also filter the alarms based on alarm type, severity, description and date.

Figure 36: View Alarms Page

View Alarms

Alarm filter

Alarm type: All

Severity: All

Description:

Date From:

To:

Go

Reset

Alarm Details

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

Part 3

Index

- Index on page 105

Index

Symbols

#, comments in configuration statements.....	xvii
(), in syntax descriptions.....	xvii
* (red asterisk).....	20
/cf/var/crash directory <i>See</i> crash files	
/cf/var/log directory <i>See</i> system logs	
/cf/var/tmp directory <i>See</i> temporary files	
< >, in syntax descriptions.....	xvii
? icon	20
[], in configuration statements.....	xvii
{ }, in configuration statements.....	xvii
(pipe), in syntax descriptions.....	xvii

A

access, configuration summary.....	55
accounting options	
configuration summary.....	55
sample task.....	62
Add button.....	49
Add new entry link.....	60
advanced BGP feature, license.....	87
alarms	
chassis.....	99
interface.....	99
major.....	100
minor.....	100
red.....	100
severity.....	100
system.....	99
type.....	99
viewing, sample.....	100
yellow.....	100
alarms sample task.....	100
alert logging severity.....	93
applications, configuration summary.....	56
Apply button.....	22, 49

B

backup	
boot device.....	89
current configuration.....	89

rescue configuration.....	89
system software.....	89
basic connectivity	
Quick Configuration.....	6
requirements.....	6
sample task.....	49
selecting.....	88
basic setup <i>See</i> setup	
braces, in configuration statements.....	xvii
brackets	
angle, in syntax descriptions.....	xvii
square, in configuration statements.....	xvii
browser interface <i>See</i> J-Web interface	
buttons	
Add (Quick Configuration).....	49
Apply (Quick Configuration).....	22, 49
Cancel (J-Web configuration editor).....	23, 61
Cancel (Quick Configuration).....	22
Commit (J-Web configuration editor).....	23, 61
Delete (Quick Configuration).....	49
Discard (J-Web configuration editor).....	61
OK (J-Web configuration editor).....	23, 61
OK (Quick Configuration).....	22
Refresh (J-Web configuration editor).....	61

C

Cancel button.....	61
J-Web configuration editor.....	23
Quick Configuration.....	22
certificates <i>See</i> SSL certificates	
chassis	
configuration summary.....	56
monitoring.....	28
chassis viewer.....	37
class of service (CoS)	
configuration summary.....	56
monitoring.....	30
Quick Configuration summary.....	48
cleaning up files.....	85
CLI <i>See</i> JUNOS CLI	
CLI terminal.....	77
overview.....	77
starting.....	79
clickable configuration <i>See</i> J-Web configuration editor	
command-line interface <i>See</i> JUNOS CLI	

comments, in configuration statements.....	xvii
Commit button.....	23, 61
committed configuration	
comparing two configurations.....	69
methods.....	68
overview.....	43, 45
rescue configuration	71
storage location.....	44, 45
summaries.....	67
committing a configuration.....	43, 45
configuration	
basic.....	47
committing	62
committing as a text file, with caution	64
discarding changes	61
downloading	70
editing	55, 58
editing as a text file, with caution	64
loading previous	71
rollback	71
uploading	65
users-editors, viewing.....	68
viewing as a text file	53
configuration database, summary.....	69
configuration hierarchy, J-Web display.....	21
configuration history	
comparing files.....	69
database summary.....	69
downloading files.....	70
summary.....	67
users-editors, viewing.....	68
Configuration History page.....	67
configuration sample tasks	
accounting options.....	62
firewall filters.....	51
setup.....	49
configuration text	
editing and committing, with caution.....	64
viewing.....	53
configure link.....	60
connectivity	
losing, after initial configuration.....	14
lost DHCP lease after initial configuration.....	7
conventions	
how to use this guide.....	xv
notice icons.....	xvi
text and syntax.....	xvi
CoS <i>See</i> class of service	
crash files, cleaning up.....	85
critical logging severity.....	93
curly braces, in configuration statements.....	xvii
customer support.....	xviii
contacting JTAC.....	xviii

D

data link switching (DLSw), license.....	87
Database Information page.....	67
debug logging severity.....	93
default gateway	
defining (Quick Configuration).....	8
Delete button.....	49
Delete Configuration Below This Point option	
button.....	62
delete link.....	60
deleting a current rescue configuration	71
DHCP (Dynamic Host Configuration Protocol)	
monitoring.....	34
Quick Configuration summary.....	48
DHCP server, regaining lost lease.....	7, 14
diagnose	
CLI terminal.....	77
network connectivity.....	73
packet capture.....	76
ping ATM.....	75
ping host.....	73
ping MPLS.....	74
traceroute.....	76
diagnose sample task.....	80
Discard All Changes option button.....	62
Discard button.....	61
Discard Changes Below This Point option button.....	62
discarding configuration changes.....	61
DNS server, defining (Quick Configuration).....	8
documentation set	
comments on.....	xviii
domain name, defining (Quick Configuration).....	7
domain search, defining (Quick Configuration).....	8
downgrading JUNOS software.....	86
downloading configuration files	70

E

Edit Configuration page.....	59
Edit Configuration Text page.....	64
edit link.....	60
editing a configuration.....	55
emergency logging severity.....	93
error logging severity.....	93
event options, configuration summary.....	56
events	
filtering.....	93
filters.....	93
overview.....	91
regular expressions for filtering.....	95
severity levels.....	92
using.....	91
viewing.....	92
viewing, sample.....	96
events sample task.....	96

F

fe-0/0/0, defining address (Quick Configuration).....	9
feature licenses <i>See</i> license	
file management	
crash files	85
log files	85
temporary files	85
filtering events	
overview.....	93
regular expressions.....	95
firewall filters	
configuration summary.....	56
monitoring.....	33
Quick Configuration summary.....	48
sample task.....	96
font conventions.....	xvi
Forwarding Engine Board redundancy	
monitoring.....	36
Quick Configuration summary.....	48
forwarding options, configuration summary.....	56
fxp0, defining address (Quick Configuration).....	9

G

ge-0/0/0, defining address (Quick Configuration).....	9
---	---

H

halting a Services Router immediately.....	88
hardware, major (red) alarm conditions on.....	100
Help icon (?).....	20, 23
Help, J-Web interface.....	19, 23
hostname, defining (Quick Configuration).....	7
how to use this guide.....	xv
HTTP (Hypertext Transfer Protocol)	
enabling Web access (Quick Configuration).....	10
on built-in management interfaces.....	9
httpd process, limiting subordinate processes.....	13
HTTPS (Hypertext Transfer Protocol over SSL)	
enabling secure access (Quick Configuration).....	10
Quick Configuration.....	10
recommended for secure access.....	9
Hypertext Transfer Protocol <i>See</i> HTTP	
Hypertext Transfer Protocol over SSL <i>See</i> HTTPS	

I

identifier link.....	60
info logging severity.....	93
initial configuration requirements.....	6
installing JUNOS software.....	86
interfaces	
configuration summary.....	56
monitoring.....	29
Quick Configuration summary.....	48

Internet Explorer, modifying for worldwide version of JUNOS software.....	4
invalid configuration, replacing.....	71
IPSec tunnels	
monitoring.....	33
Quick Configuration summary.....	48

J

J-flow traffic analysis, license.....	87
J-Web configuration editor	
committing a configuration.....	62
configuration hierarchy display.....	21
configuration text, viewing.....	53
editing a configuration.....	58
J-Web interface	
comparing configuration differences.....	69
context-sensitive help.....	19
event viewer.....	96
Help (?) icon.....	20
Internet Explorer, modifying for worldwide version of JUNOS software.....	4
layout.....	19
losing connectivity after initial configuration.....	14
main pane.....	20
overview.....	17, 43
page layout.....	18
side pane.....	21
starting.....	4
top pane.....	19
unpredictable results, multiple windows.....	14
J-Web Quick Configuration <i>See</i> Quick Configuration	
J-Web software, installing.....	3
JUNOS CLI.....	77
command modes.....	77
overview.....	77
<i>See also</i> CLI terminal	
JUNOS software	
downgrading.....	86
installing.....	86
Internet Explorer, modifying for worldwide version.....	4
release notes, URL.....	xiv
upgrading.....	86
worldwide version, modifying Internet Explorer for.....	4
JUNOScript API	
defining access (Quick Configuration).....	9
enabling secure access.....	10
JUNOScript over SSL.....	10
L	
layout, J-Web.....	19

license	
add.....	87
advanced BGP feature.....	87
data link switching (DLSw).....	87
delete.....	87
display keys.....	87
J-flow traffic analysis.....	87
manage.....	87
limitations	
software downgrade cannot be undone.....	87
unpredictable behavior with multiple windows.....	14
loading a configuration file	
downloading	70
rollback	71
uploading	65
Locate LSP from virtual circuit information.....	75
Locate LSP using interface name.....	75
logging severity levels.....	93
loopback address, defining (Quick Configuration).....	8

M

main pane, J-Web.....	20
major (red) alarms.....	100
management access, sample task.....	51
management device	
monitoring from.....	27
management interface address, defining (Quick Configuration).....	9
manuals	
comments on.....	xviii
minor (yellow) alarms.....	100
monitor sample task.....	38, 40
monitoring	
chassis.....	28
chassis viewer.....	37
class of service.....	30
CLI commands and corresponding J-Web options.....	27
DHCP.....	34
FEB redundancy.....	36
firewall filters.....	33
interfaces.....	29
interfaces, sample.....	38
IPSec.....	33
J-Web tasks and corresponding CLI commands.....	27
MPLS.....	31
NAT.....	34
overview.....	27
<i>See also</i> diagnosis; statistics; status	
PPPoE.....	36
route information, sample.....	40
routing.....	29
RPM.....	35

service sets.....	32
system.....	28
MPLS, monitoring.....	31

N

NAT (Network Address Translation)	
monitoring.....	34
Quick Configuration summary.....	48
network access, sample task.....	51
Network Address Translation <i>See</i> NAT	
network connectivity.....	73
notice icons.....	xvi
notice logging severity.....	93
NTP server, defining (Quick Configuration).....	8

O

OK button.....	61
J-Web configuration editor.....	23
Quick Configuration.....	22
openssl command.....	9
option buttons	
Delete Configuration Below This Point.....	62
Discard All Changes.....	62
Discard Changes Below This Point.....	62

P

packet capture.....	76
pages, layout in J-Web.....	18
parentheses, in syntax descriptions.....	xvii
partition, storage medium.....	89
ping	
ATM.....	75
host.....	73
MPLS.....	74
ping host	
results.....	82
sample.....	80
ping MPLS	
layer-2 VPN, instance.....	74
layer-2 VPN, interface.....	74
LDP-signaled LSP.....	74
LSP endpoint.....	74
LSP to Layer 3 VPN prefix.....	74
options.....	46
RSVP-signaled LSP.....	74
policy options, configuration summary.....	56
PPPoE, monitoring.....	36

Q

Quick Configuration	
basic settings.....	6
buttons.....	22, 49

- initial configuration.....6
 - overview.....47
 - Secure Access page.....11
 - secure Web access.....10
- R**
- radio buttons *See* option buttons
 - real-time performance monitoring *See* RPM
 - reboot immediately88
 - red asterisk (*).....20
 - Refresh button.....61
 - regaining DHCP lease after initial configuration.....7
 - regular expressions for filtering events.....95
 - release notes, URL.....xiv
 - required entry20
 - rescue configuration
 - deleting71
 - setting71
 - viewing71
 - rolling back a configuration file during
 - configuration.....71
 - root password, defining (Quick Configuration).....8
 - route information sample task.....40
 - routing instances, configuration summary.....57
 - routing options, configuration summary.....57
 - routing protocols
 - configuration summary.....57
 - Quick Configuration summary.....48
 - routing, monitoring.....29
 - RPM (real-time performance monitoring)
 - graph results.....35
 - monitoring.....35
 - Quick Configuration summary.....48
 - RPM probes.....35
 - sample graphs.....35
- S**
- sample tasks
 - configuring accounting options.....62
 - configuring firewall filters.....51
 - configuring setup.....49
 - filtering and viewing events.....96
 - managing snapshots.....90
 - monitoring interfaces.....38
 - monitoring route information.....40
 - ping host.....80
 - viewing alarms.....100
 - scheduling a reboot.....88
 - secure access
 - generating SSL certificates.....9
 - HTTPS access (Quick Configuration).....10
 - HTTPS recommended.....9
 - installing SSL certificates (Quick Configuration).....10
 - JUNOScript SSL access.....10
 - Quick Configuration summary.....48
 - Secure Access page
 - description.....10, 11
 - field summary.....12
 - security, configuration summary.....57
 - service sets, monitoring.....32
 - services, configuration summary.....57
 - sessions
 - limiting number of.....13
 - limits.....13
 - terminating.....13
 - Set Up page
 - field summary.....7
 - prerequisites.....6
 - setup
 - Quick Configuration.....6
 - requirements.....6
 - sample task.....49
 - severity levels for events.....93
 - side pane, J-Web.....21
 - snapshot
 - sample task.....90
 - system software.....89
 - SNMP
 - configuration summary.....57
 - Quick Configuration summary.....48
 - software package
 - downgrading.....86
 - installing.....86
 - upgrading.....86
 - software, halting immediately.....88
 - SSH, defining access (Quick Configuration).....9
 - SSL (Secure Sockets Layer)
 - enabling secure access (Quick Configuration).....10
 - SSL 3.0 option, disabling on Internet Explorer for
 - worldwide version of JUNOS software.....4
 - SSL certificates
 - adding (Quick Configuration).....12
 - generating.....9
 - startup, J-Web interface.....4
 - Summary Quick Configuration page.....47
 - support, technical *See* technical support
 - syntax conventions.....xvi
 - system
 - configuration summary.....57
 - monitoring.....28
 - Quick Configuration summary.....48
 - system log messages
 - displaying at a terminal (configuration editor).....95
 - filtering (Quick Configuration).....93
 - overview.....91
 - system logs
 - enabling.....97
 - file cleanup85
 - functions.....91

logging severity levels.....	93
messages <i>See</i> system log messages	
system management	
files.....	85
licenses.....	87
reboots.....	88
software.....	86
system time	
defining (Quick Configuration).....	8
synchronizing (Quick Configuration).....	8

T

taskbar.....	19
technical support	
contacting JTAC.....	xviii
Telnet, defining access (Quick Configuration).....	9
temporary files, cleaning up.....	85
time to live <i>See</i> TTL	
time zone, defining (Quick Configuration).....	8
timeout sessions.....	13
top pane, J-Web.....	19
traceroute, overview.....	76
troubleshooting	
events.....	97
J-Web access.....	14
J-Web behavior.....	14
router connectivity.....	14
TTL (time to live), ping requests.....	82

U

unknown logging severity.....	93
upgrading JUNOS software.....	86
uploading a configuration file.....	65
URLs, release notes.....	xiv
user interfaces	
preparation.....	4
users	
Quick Configuration summary.....	48
viewing.....	14
using alarms tasks.....	99

V

view and edit	
committing a text file, with caution.....	64
configuration text, viewing.....	53
configuration, editing.....	55
uploading a file.....	65
View Configuration Text page.....	54
View Events page	
field summary (filtering log messages).....	94
overview.....	91
viewing alarms, sample task.....	100
viewing configuration text.....	53

viewing events, sample task.....	96
----------------------------------	----

W

warning logging severity.....	93
Web access, secure <i>See</i> secure access	
Web browser, modifying Internet Explorer for worldwide version of JUNOS software.....	4
windows, J-Web, unpredictable results with multiple.....	14

Y

yellow alarms.....	100
--------------------	-----