



JUNOS™ Internet Software

Software Installation and Upgrade Guide

Release 8.2

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-017608-01, 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.

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

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

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

Copyright © 2007, Juniper Networks, Inc.
All rights reserved. Printed in USA.

JUNOS Internet Software Installation and Upgrade Guide, Release 8.2

Writing: Donice G. Mitchell
Editing: Nancy Kurahashi
Illustration: Faith Bradford
Cover design: Edmonds Design

Revision History
12 January 2007—Revision 1

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

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.

Year 2000 Notice

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

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

End User License Agreement

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

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.

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

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

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

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

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

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

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

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

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

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

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

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

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

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

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

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

	About This Guide	vii
	Objectives	vii
	Supported Routing Platforms	viii
	Audience	viii
	Using the Examples in This Manual.....	ix
	Merging a Full Example	ix
	Merging a Snippet.....	x
	Documentation Conventions.....	x
	Related Juniper Networks Documentation.....	xii
	Documentation Feedback	xv
	Requesting Support.....	xv
Chapter 1	JUNOS Software Media and Packages	1
	JUNOS Software Versions.....	2
	FIPS 140-2 Security Compliance	2
	JUNOS Software Release Numbers	3
	JUNOS Software Installation Packages.....	3
	Individual Software Packages Within jinstall and jbundle	4
	Software Package Information Security.....	4
	Storage Media	5
	Boot Devices	5
	Boot Sequence	6
Chapter 2	Configuring JUNOS Software	7
	Configuring the Software from External Devices.....	7
	Methods for Configuring JUNOS Software	8
	JUNOS Command-Line Interface (CLI)	9
	J-Web Package.....	9
	JUNOScript API Software	9
	NETCONF API Software	10
	Configuration Commit Scripts.....	10
	Configuring a Router for the First Time.....	10
	Configuring a Router with Dual Routing Engines for the First Time	14
	JUNOS Software Default Settings That Protect the Router	16
	Configuring Software Properties	17
	Activating a Configuration	17
	Managing Available Disk Space	17
	Using Software Monitoring Tools.....	18
	Router Security	19
	Router Access	19
	User Authentication	20
	Specifying Plain-Text Passwords.....	21
	Routing Protocol Security Features	22
	Firewall Filters	22
	Auditing for Security	22

Chapter 3	Installing a Different JUNOS Software Version on a Router	25
	Confirming that Current Configuration Is Compatible with the Candidate Software	26
	Verifying PIC Combinations	26
	Determining Which JUNOS Software Version Is Running	27
	Upgrading All Software Packages	27
	Upgrading Individual Software Packages.....	31
	Installing the JUNOS Software on Routers with Redundant Routing Engines.....	32
Chapter 4	Reinstalling the Software Using jinstall	35
Chapter 5	Reinstalling the JUNOS Software From Removable Media	39
	Preparing to Reinstall the JUNOS Software.....	39
	Reinstalling the JUNOS Software	40
	Restoring the Saved Configuration	40
	Index.....	43

About This Guide

This preface provides the following guidelines for using the *JUNOS Internet Software Installation and Upgrade Guide* and related Juniper Networks, Inc., technical documents:

- Objectives on page vii
- Supported Routing Platforms on page viii
- Audience on page viii
- Merging a Full Example on page ix
- Documentation Conventions on page x
- Related Juniper Networks Documentation on page xii
- Documentation Feedback on page xv
- Requesting Support on page xv

Objectives

This guide provides a description of JUNOS software packaging and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software.



NOTE: This guide documents Release 8.2 of the JUNOS Internet software. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at <https://www.juniper.net/>.

Supported Routing Platforms

For the features described in this manual, the JUNOS software currently supports the following routing platforms:

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

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks routing platform.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

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.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the `load merge` or the `load merge relative` command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the `load merge` command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```

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

```

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

```

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

```

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the `load` command, see the *JUNOS CLI User Guide*.

Documentation Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons



Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.

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

Table 2: Text and Syntax Conventions (1 of 2)

Convention	Element	Example
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width typeface	Represents output on the terminal screen.	user@host> show chassis alarms No alarms currently active

Table 2: Text and Syntax Conventions (2 of 2)

Convention	Element	Example
<i>Italic typeface</i>	<ul style="list-style-type: none"> ■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> ■ A policy <i>term</i> is a named structure that defines match conditions and actions. ■ <i>JUNOS System Basics Configuration Guide</i> ■ RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic sans serif typeface</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Sans serif typeface	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> ■ To configure a stub area, include the stub statement at the [edit protocols ospf area <i>area-id</i>] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold typeface	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

Related Juniper Networks Documentation

Table 3 lists the software and hardware guides and release notes for the supported Juniper Networks routing platforms and describes the contents of each document. Table 4 lists the books included in the *Network Operations Guide* series.

Table 3: Technical Documentation for Supported Routing Platforms (1 of 3)

Document	Description
JUNOS Internet Software Configuration Guides	
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Internet software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
<i>Software Installation and Upgrade Guide</i>	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.

Table 3: Technical Documentation for Supported Routing Platforms (2 of 3)

Document	Description
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing protocols and policies, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as CoS, IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web GUI to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
JUNOS Comprehensive Index and Glossary	
<i>Comprehensive Index and Glossary</i>	Provides a complete index of all JUNOS software books, the <i>JUNOScript API Guide</i> , and the <i>NETCONF API Guide</i> . Also provides a comprehensive glossary.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software GUI, how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
J-series Services Router Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the <i>Getting Started Guide</i> for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.

Table 3: Technical Documentation for Supported Routing Platforms (3 of 3)

Document	Description
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform PICs. Each platform has its own PIC guide.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and the supported PICs, and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Software Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>J-series Services Router Release Notes</i>	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 4: JUNOS Internet Software Network Operations Guides

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

Documentation Feedback

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

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

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

Chapter 1

JUNOS Software Media and Packages

Your routing platform comes with JUNOS software installed on it. When you power on the router, all software starts automatically. You simply need to configure the software so that the router will be ready to participate in the network.

The software is installed on the router's flash disk (a nonrotating drive) and hard disk (a rotating disk). A copy of the software also is provided on removable media, either a PC Card, which can be inserted into the router's drive or card slot. By default, when you power on the router, it runs the copy of the software that is installed on the flash disk.

You can upgrade the router software as new features are added or software problems are fixed. You normally obtain new software by downloading the images from the Juniper Support Web page onto your router or onto another system on your local network. Then you install the software upgrade on the router's flash disk and hard disk. You can also copy the software onto the removable media.

Juniper Networks routing platforms run only binaries supplied by Juniper Networks. Each JUNOS software image includes a digitally signed manifest of executables, which are registered with the system only if the signature can be validated. JUNOS software will not execute any binary without a registered fingerprint. This feature protects the system against unauthorized software and activity that might compromise the integrity of your router.



NOTE: JUNOS Release 7.2 and later releases include a digitally signed manifest of executables. JUNOS Release 7.5 and later releases require these signed manifests to enable execution of binaries.

This chapter discusses the following topics:

- JUNOS Software Versions on page 2
- JUNOS Software Release Numbers on page 3
- JUNOS Software Installation Packages on page 3
- Individual Software Packages Within jinstall and jbundle on page 4
- Software Package Information Security on page 4
- Storage Media on page 5

- Boot Devices on page 5
- Boot Sequence on page 6

JUNOS Software Versions

You can download the JUNOS software from the Juniper Networks Support Web page by selecting one of the following editions:

- Canada and U.S.—JUNOS software for customers in the United States and Canada. This edition includes high-encryption capabilities for data leaving the router.
- Worldwide—JUNOS software for all other customers. This edition does not include any high-encryption capabilities for data leaving the router.
- JUNOS-FIPS—JUNOS software which provides advanced network security for customers who need software tools to configure a network of Juniper Networks routers in a Federal Information Processing Standards (FIPS) 140-2 environment. For more information about JUNOS-FIPS, see “FIPS 140-2 Security Compliance” on page 2.

FIPS 140-2 Security Compliance

For advanced network security, a special version of JUNOS, called JUNOS-FIPS 140-2, is available. JUNOS-FIPS 140-2 provides customers with software tools to configure a network of Juniper Networks routers in a FIPS environment. FIPS support includes:

- Upgrade package to convert JUNOS to JUNOS-FIPS 140-2
- Revised installation and configuration procedures
- Enforced security for remote access
- FIPS user roles (Crypto Officer, User, and Maintenance)
- FIPS-specific system logging and error messages
- IPSec configuration for Routing Engine-to-Routing Engine communication
- Enhanced password creation and encryption



NOTE: JUNOS-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If JUNOS-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

JUNOS-FIPS has special installation and configuration requirements. Installation procedures include downloading the FIPS software package from www.juniper.net. For detailed guidelines on how installation and configuration procedures differ between JUNOS and JUNOS-FIPS 140-2, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

JUNOS Software Release Numbers

The JUNOS software release number represents a particular revision of the software that runs on a Juniper Networks routing platform, for example, JUNOS 7.5, 7.6 or 8.0. Each JUNOS software release has certain new features that compliment the software processes that support Internet routing protocols, control the router's interfaces and the router chassis itself, and allow router system management. On the Juniper Support Web page, you select to download JUNOS software for a particular JUNOS software release number.

The software release number is also reflected in the installation package filename. The following is an example of how the software release name is formatted in the installation package filename:

```
jinstall-JUNOS-m.nZx.x-domestic-signed.tgz
```

```
jinstall-8.0R1.10-domestic-signed.tgz
```

m.n is two integers that represent the software release number; *m* denotes the major release number.

Z is a capital letter that indicates the type of software release. In most cases, it is an *R*, to indicate that this is released software. If you are involved in testing prereleased software, this letter might be an *A* (fore alpha-level software), *B* (for beta-level software), or *I* (a capital letter *I*; for internal test, or experimental versions of software).

x.x is the software build number and spin number.

JUNOS Software Installation Packages

The JUNOS software from the Juniper Support Web page provides three installation packages. A *package* is a collection of files that make up a software component.

- **Install Package—jinstall**—A package used to upgrade from JUNOS Release 7.x to 8.x or 8.x to 8.x when the software becomes damaged. If you upgrade from 7.x to 8.x using **jinstall**, use **jbundle** for subsequent upgrades or downgrades. The **jinstall** package completely reinstalls the software. It rebuilds the JUNOS file system only and retains configuration information from the previous version. However, logs and other types of auxiliary information may be erased during installation. For more information about installing the JUNOS software using the **jinstall** package, see “Reinstalling the Software Using jinstall” on page 35.

- **Software Bundle—`jbundle`**—A package used to downgrade from Release 8.x. `jbundle` is also used to upgrade or downgrade between minor versions of the JUNOS software. `jbundle` modifies the smallest set of files needed to change to the new software version. Use the `jbundle` package only when instructed by a Juniper Networks support representative.



NOTE: You cannot use the `jbundle` package to upgrade from JUNOS 5.x to JUNOS 7.x. For more information about how to upgrade from Release 5.x or later to 7.x or later, see the Knowledge Base Asset # 24602 on the Juniper Networks Support Web site at <http://www.juniper.net/support>.

- **J-Series Install Bundle—`junos-jseries`**—A package used to install the JUNOS-J-series software on J-series Services routing platforms. `jweb`, the J-Web package within this bundle and the `jinstall` and `jbundle` packages contains the J-Web graphical user interface software for managing J-series, M-series, and T-series routing platforms.

Individual Software Packages Within `jinstall` and `jbundle`

The `jinstall` and `jbundle` packages consists of the following individual packages:

- `kernel`—Kernel and network tools package, which contains the operating system.
- `base`—Base package, which contains additions to the operating system.
- `route`—Routing package, which contains the software that runs on the Routing Engine.
- `pf`—Software that runs on the Packet Forwarding Engine.
- `docs`—Documentation package, which contains the documentation for the software.
- `crypto`—Encryption package, which contains security software (domestic version).
- `jweb`—J-Web package, which contains the graphical user interface software for J-series, M-series, and T-series routing platforms.

Software Package Information Security

All JUNOS software is delivered in signed packages that contain digital signatures, Secure Hash Algorithm (SHA-1), and Message Digest 5 (MD5) checksums. A package is installed only if the checksum within it matches the hash recorded in its corresponding file. Which checksum is used depends on the software version:

- Digital signatures are used when you upgrade or downgrade between JUNOS Release 7.0 and a later version.
- The SHA-1 checksum is used when you upgrade or downgrade between JUNOS Release 6.4 and a later version.

- The MD5 checksum is used when you upgrade or downgrade between JUNOS Release 6.3 or earlier and a later version.

Storage Media

The router has three forms of storage media, and each comes with JUNOS system software preinstalled:

- Flash disk, which is a nonrotating drive.
- Hard disk, which is a rotating drive. This drive also is used to store system log files and diagnostic dump files.
- Removable media, either a PC Card or an LS-120 floppy disk.

Table 5 specifies the storage media names by Routing Engine. The storage media device names are displayed when the router boots.

Table 5: Device Names

Device	Flash Disk	Hard Disk	Removable Media
Routing Engine 200 (RE-M40) (CLI name = RE1)	ad0	ad2	adf0
Routing Engine 333 (CLI name = RE2)	ad0	ad1	ad3
Routing Engine 600 (CLI name = RE3)	ad0	ad1	ad3
Routing Engine 1600 (CLI name = RE4)	ad0	ad1	ad3 and ad4
Routing Engine 400 (CLI name = RE5)	ad0	ad1	ad3

Boot Devices

The router can boot from the flash disk, the hard disk, or a removable medium. The disk from which the router boots is called the *primary boot device*, and the other disk is the *alternate boot device*.



NOTE: If the router boots from an alternate boot device, a yellow alarm lights the LED on the router's craft interface.

Boot Sequence

The router attempts to boot from three devices in this order:

- Removable medium, if one is installed
- Flash disk
- Hard disk

Most router models normally boot from the flash disk. The M7i router is not always shipped with a flash disk, and normally boots from a removable PC Card installed in a slot in its Routing Engine.



NOTE: To reinstall the JUNOS software, you boot the router from the removable media. Do not insert the removable media during normal operations. The router does not operate normally when it is booted from the removable media.

When the router boots from the storage media (flash disk, hard disk, or removable media) it expands its search in the `/config` directory of the routing platform for the following files in the following order: `juniper.conf` (the main configuration file), `rescue.conf` (the rescue configuration file), and `juniper.conf.1` (the first rollback configuration file). When the search finds the first configuration file that can be loaded properly, the file loads and the search ends. If none of the files can be loaded properly, the routing platform does not function properly.

If the router boots from an alternate boot device, the JUNOS software displays a message indicating this when you log in to the router. For example, this message shows that the software booted from the hard disk (`/dev/ad2s1a`):

```
login: username
Password: password
Last login: date on terminal

– JUNOS 8.0 R1 built date
–
– NOTICE: System is running on alternate media device (/dev/ad2s1a).
```

The default boot order for the M7i Internet router is different from other Juniper Networks routers, because the default configuration of the Routing Engine on the M7i router does not include an internal compact flash disk.

If the Routing Engine does not have an internal compact flash disk, two copies of the JUNOS software are preinstalled on the router: one on a PC Card that can be inserted into the slot in the Routing Engine faceplate, and one on a rotating hard disk in the Routing Engine. When the router boots, it first attempts to access the software image on the PC Card. If a PC Card is not inserted into the Routing Engine or the attempt otherwise fails, the router tries the hard disk.

If the Routing Engine has an internal compact flash disk, three copies of the JUNOS software are preinstalled on the router. When the router boots, it first attempts to access the image on the PC Card. If a PC Card is not inserted into the Routing Engine or the attempt otherwise fails, the router next tries the flash disk, and finally the hard disk.

Chapter 2

Configuring JUNOS Software

To configure the JUNOS software, you must specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as some system hardware properties. After you have created a candidate configuration, you commit the configuration to be evaluated and activated by the JUNOS software.

This chapter discusses the following topics:

- Configuring the Software from External Devices on page 7
- Methods for Configuring JUNOS Software on page 8
- Configuring a Router for the First Time on page 10
- Managing Available Disk Space on page 17
- Using Software Monitoring Tools on page 18
- Router Security on page 19

Configuring the Software from External Devices

You can configure the router from a system console connected to the routing platform's console port or by using Telnet to access the router remotely. The router provides three ports on the craft interface for connecting external management devices to the Routing Engine and the JUNOS software:

- Console port—Connects a system console using an RS-232 serial cable.
- Auxiliary port—Connects a laptop or modem using an RS-232 serial cable.
- Ethernet management port—Connects the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for remote management through a PC or other client device. The Ethernet port is 10/100 megabits-per-second (Mbps) autosensing and requires an RJ-45 connector.

Methods for Configuring JUNOS Software

You can use any of the methods shown in Table 6 to configure JUNOS system software:

Table 6: Methods for Configuring JUNOS Software

Method	Description
Command-line interface (CLI)	Create the configuration for the router using the CLI. You can enter commands from a single command line, and scroll through recently executed commands.
ASCII file	Load an ASCII file containing a router configuration that you created earlier, either on this system or on another system. You can then activate and run the configuration file, or you can edit it using the CLI and then activate it.
J-Web graphical user interface (GUI)	Use the J-Web graphical user interface (GUI) to configure the router. J-Web allows you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser. The J-Web GUI is preinstalled on J-series Services Routers and is an optional software package that can be installed on M-series and T-series routers.
JUNOScript application programming interface (API)	Use JUNOScript Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use the JUNOScript API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The JUNOScript API is customized for JUNOS software and operations in the API are equivalent to JUNOS CLI.
NETCONF application programming interface (API)	Use NETCONF Perl client modules to develop custom applications for configuring information on routing platforms that run JUNOS software. Client applications use NETCONF API to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. The NETCONF API includes features that accommodate the configuration data models of multiple vendors.
Configuration commit scripts	Create scripts that run at commit time to enforce custom configuration rules. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT).

This section contains complete descriptions of each method you can use to configure JUNOS system software:

- JUNOS Command-Line Interface (CLI) on page 9
- J-Web Package on page 9
- JUNOScript API Software on page 9
- NETCONF API Software on page 10
- Configuration Commit Scripts on page 10

JUNOS Command-Line Interface (CLI)

The JUNOS CLI is a straightforward command interface. You use Emacs-style keyboard sequences to move around on a command line and scroll through a buffer that contains recently executed commands. You type commands on a single line, and the commands are executed when you press the **Enter** key. The CLI also provides command help and command completion. For more information about the CLI, see the *JUNOS CLI User Guide* and *JUNOS System Basics and Services Command Reference*.

J-Web Package

As an alternative to entering CLI commands, JUNOS supports a J-Web graphical user interface (GUI). The J-Web user interface allows you to monitor, configure, troubleshoot, and manage the router on a client by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

The J-Web user interface is preinstalled on J-series Services Routers. It is provided as an optional, licensed software package (**jweb** package) on M-series and T-series routing platforms. The **jweb** package is not included in **jinstall** and **jbundle** software bundles. It must be installed separately. To install the package on M-series and T-series routing platforms, follow the procedure described in “Upgrading Individual Software Packages” on page 31.

J-Web supports weak (56-bit) encryption by default. This enables international customers to install J-Web and use HTTPS connections for J-Web access. Domestic customers can also install the **crypto** strong encryption package. This package automatically overrides the weak encryption. For more information about the J-Web GUI, see the *J-Web Interface User Guide*.



NOTE: Because the J-Web package is bundled separately from other packages, it is possible to have a version mismatch between J-Web and other JUNOS software packages you have installed.

To check for a version mismatch, use the **show system alarms** CLI command. If the version number does not match exactly, a system alarm appears. For example, if you install the 7.4R1.2 **route** package and the 7.4R1.1 **jweb** package, an alarm is activated. For more information on the **show system alarms** command, see the *JUNOS System Basics and Services Command Reference*.

JUNOScript API Software

The JUNOScript API is an Extensible Markup Language (XML) application that client applications use to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. This API is customized for JUNOS software, and operations in the API are equivalent to JUNOS CLI configuration mode commands. The JUNOScript API includes a set of Perl modules that enable client applications to communicate with a JUNOScript server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and JUNOScript API software, see the *JUNOScript API Guide*.

NETCONF API Software

The NETCONF API is an Extensible Markup Language (XML) application that client applications can use to request and change configuration information on Juniper Networks J-series, M-series, and T-series routing platforms. This API is customized for JUNOS software, and includes features that accommodate the configuration data models of multiple vendors. The NETCONF API includes a set of Perl modules that enable client applications to communicate with a NETCONF server on the router. The Perl modules are used to develop custom applications for configuring and monitoring JUNOS software.

For a complete description of how to use JUNOS XML and NETCONF API software, see the *NETCONF API Guide*.

Configuration Commit Scripts

You can create and use scripts that run at commit time to enforce custom configuration rules. If a configuration breaks the custom rules, the script can generate actions that the JUNOS software performs. These actions include:

- Generating custom error messages
- Generating custom warning messages
- Generating custom system log messages
- Making changes to the configuration

Configuration commit scripts also enable you to create macros, which expand simplified custom aliases for frequently used configuration statements into standard JUNOS configuration statements. Commit scripts are written in Extensible Stylesheet Language Transformations (XSLT). For more information, see the *JUNOS Configuration and Diagnostic Automation Guide*.

Configuring a Router for the First Time

On most JUNOS routing platforms, the JUNOS software is installed on the flash disk and on the hard disk. When you first turn on a routing platform, it runs the version of the JUNOS software installed on the flash. The copy of JUNOS software on the hard disk is a backup. Another backup copy of the JUNOS software is available on removable media, such as a PC Card or a compact flash card. Be sure to put the backup JUNOS software (on removable media) in a safe place.

When you turn on a routing platform the first time, the JUNOS software automatically boots and starts. You must enter basic configuration information so that the routing platform is on the network and you can log in to it over the network.

To configure the routing platform initially, you must connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default. Remote management access to the routing platform and all management access protocols, including Telnet, FTP, and SSH, are disabled by default.

When you first connect to the routing platform console, you must log in as the user **root**. At first, the root account requires no password. You see that you are the user **root**, because the routing platform command prompt shows the username **root@#**.

You must start the JUNOS software command-line interface (CLI) using the command **cli**. The command prompt **root@>** indicates that you are the user **root** and that you are in the JUNOS software operational mode. Enter the JUNOS software configuration mode by typing the command **configure**. The command prompt **root@#** indicates that you are in the JUNOS software configuration mode.

When you first configure a routing platform, you must configure the following basic properties:

- Routing platform hostname
- Domain name
- IP address of the routing platform Ethernet management interface—**fxp0**
- IP address of a backup router
- The IP address of one or more DNS name servers on your network
- Password for the root account

To configure the software for the first time, follow these steps:

1. Connect a terminal or laptop computer to the routing platform through the console port—a serial port on the front of the routing platform. Only console access to the routing platform is enabled by default.
2. Power on the routing platform and wait for it to boot.

The JUNOS software boots automatically. The boot process is complete when you see the **login:** prompt on the console.

3. Log in as the user **root**.

Initially, the **root** user account requires no password. You can see that you are the **root** user, because the prompt on the routing platform shows the username **root@#**.

4. Start the JUNOS software command-line interface (CLI):

```
root@# cli
root@>
```

5. Enter JUNOS software configuration mode:

```
cli> configure
[edit]
root@#
```

6. Configure the name of the routing platform (the routing platform hostname). We do not recommend spaces in the routing platform name. However, if the name does include spaces, enclose the entire name in quotation marks (" ").

```
[edit]
root@# set system host-name host-name
```

7. Configure the routing platform's domain name:

```
[edit]
root@# set system domain-name domain-name
```

8. Configure the IP address and prefix length for the router management Ethernet interface, `fxp0`. `fxp0` is an Ethernet management interface that provides a separate out-of-band management network for the router.

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

9. Configure the IP address of a backup or default routing platform. This device is called the backup router, because it is used only while the routing protocol process is not running. Choose a router that is directly connected to the local routing platform by way of the management interface. The routing platform uses this backup router only when it is booting and only or when the JUNOS routing software (the routing protocol process, `rpd`) is not running.

For routing platforms with two Routing Engines, the backup Routing Engine, **RE1**, uses the backup router as a default gateway after the routing platform boots. This enables you to access the backup Routing Engine. (**RE0** is the default master Routing Engine.)

```
[edit]
root@# set system backup-router address
```

10. Configure the IP address of a DNS server. The routing platform uses the DNS name server to translate hostnames into IP addresses.

```
[edit]
root@# set system name-server address
```

11. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string. For more information about passwords, see "Specifying Plain-Text Passwords" on page 21.

Choose one of the following:

- a. To enter a clear-text password, use the following command:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

- b. To enter a password that is already encrypted, use the following command:

```
[edit]
root@# set system root-authentication encrypted-password
      encrypted-password
```

- c. To enter an SSH public key, use the following command:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

12. Optionally, display the configuration statements:

```
[edit]
root@ show
system {
  host-name host-name;
  domain-name domain.name;
  backup-router address;
  root-authentication {
    (encrypted-password "password" | public-key);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
  name-server {
    address;
  }
}
interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address address;
      }
    }
  }
}
}
```

13. Commit the configuration, which activates the configuration on the routing platform:

```
[edit]
root@# commit
```

After committing the configuration, you see the newly configured host name appear after the username in the prompt—for example, `user@host#`.

JUNOS software defaults are now set on the routing platform.

If you want to configure additional JUNOS software properties at this time, remain in the CLI configuration mode and add the necessary configuration statements. For more information about how to configure additional properties, see “Configuring Software Properties” on page 17 and the *JUNOS System Basics Configuration Guide*. You will need to commit your configuration changes to activate them on the routing platform.

14. Exit from the CLI configuration mode.

```
[edit]
root@host-name# exit
root@host-name>
```

15. Back up the configuration on the hard drive.

After you have installed the software on the routing platform, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the **request system snapshot** command to back up the new software to the `/altconfig` file system. If you do not issue the **request system snapshot** command, the configuration on the alternate boot device will be out of sync with the configuration on the primary boot device.

The **request system snapshot** command causes the root file system to be backed up to `/altroot`, and `/config` to be backed up to `/altconfig`. The root and `/config` file systems are on the routing platform's flash disk, and the `/altroot` and `/altconfig` file systems are on the routing platform's hard disk.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

Configuring a Router with Dual Routing Engines for the First Time

If a routing platform has dual Routing Engines, you must initially configure each routing platform independently. The sequence is irrelevant.

Configure the hostnames and addresses of the two Routing Engines using configuration groups in the `[edit groups]` hierarchy level. Use the reserved configuration group `re0` for the Routing Engine in slot 0 and `re1` for the Routing Engine in slot 1 to define properties specific to the individual Routing Engines. Configuring `re0` and `re1` groups lets both Routing Engines use the same configuration file.

Use the `apply-groups` statement to reproduce the configuration group information in the main part of the configuration.

The `commit synchronize` command commits the same configuration on both Routing Engines. The command makes the active or applied configuration the same for both Routing Engines with the exception of the groups, `re0` being applied to only `RE0` and `re1` being applied only to `RE1`. If you do not synchronize the configurations between two Routing Engines and one of them fails, the routing platform may end up in a very dysfunctional state since the backup Routing Engine may have a different configuration.

To initially configure a routing platform with dual Routing Engines, follow these steps in “Configure the First Routing Engine” on page 15 and “Configure the Second Routing Engine” on page 16.

Configure the First Routing Engine

1. Go to “Configuring a Router for the First Time” on page 10 and follow Steps 1 to 12 to initially configure the backup Routing Engine.
2. Instead of Step 6 and Step 8 in “Configuring a Router for the First Time” on page 10, configure a hostname for each Routing Engine and an IP address for each fxp0 management Ethernet interface as follows.

```
[edit]
root@# edit groups
[edit groups]
root@# set re0 system host-name router1
root@# set re0 interfaces fxp0 unit 0 family inet address 10.10.10.1/24
root@# set re0 system host-name router2
root@# set re1 interfaces fxp0 unit 0 family inet address 10.10.10.2/24
```

3. Set the loopback interface address for each Routing Engine.

```
[edit groups]
root@# set re0 interfaces lo0 unit 0 family inet address 2.2.2.1/32
root@# set re1 interfaces lo0 unit 0 family inet address 2.2.2.2/32
```

4. Configure the `apply-groups` statement to reproduce the configuration group information to the main part of the configuration.

```
[edit groups]
root@# top
[edit]
root@# set apply-groups [re0 re1]
```

5. Configure Routing Engine redundancy.

```
[edit]
root@# set chassis redundancy routing-engine 0 master
root@# set chassis redundancy routing-engine 1 backup
root@# set chassis redundancy routing-engine graceful-switchover enable
```

6. Save the configuration change on both Routing Engines.

```
[edit]
user@host> commit
root@#
```

7. After you have installed the new software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software on both master and backup Routing Engines.

```
{master}
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the routing platform's flash disk, and the `/altroot` and `/altconfig` file systems are on the routing platform's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy, and backup copy of the software are identical.

Configure the Second Routing Engine

Connect to the second Routing Engine and repeat the steps in “Configure the First Routing Engine” on page 15 to configure the second Routing Engine.

JUNOS Software Default Settings That Protect the Router

The following JUNOS default software settings protect against common router security weaknesses:

- The JUNOS software does not forward directed broadcast messages. Directed broadcast services send ping requests from a spoofed source address to a broadcast address and can be used to attack other Internet users. For example, if broadcast ping messages were allowed on the `200.0.0.0/24` network, a single ping request could result in up to 254 responses to the supposed source of the ping. The source would actually become the victim of a denial-of-service (DoS) attack.
- Only console access to the router is enabled by default. Remote management access to the router and all management access protocols, including Telnet, FTP, and SSH (Secure Shell), are disabled by default.
- The JUNOS software does not support the SNMP set capability for editing configuration data. While the software supports the SNMP set capability for monitoring and troubleshooting the network, this support exposes no known security issues. (You can configure the software to disable this SNMP set capability.)
- The JUNOS software ignores martian addresses that contain the following prefixes: `0.0.0.0/8`, `127.0.0.0/8`, `128.0.0.0/16`, `191.255.0.0/16`, `192.0.0.0/24`, `223.255.55.0/24`, and `240.0.0.0/4`. Martian addresses are reserved host or network addresses about which all routing information should be ignored.

Configuring Software Properties

After completing the initial minimal configuration, you can configure software properties. If you configure the software interactively using the CLI, you enter software configuration statements to create a candidate configuration that contains a hierarchy of statements. At any hierarchy level, you generally can enter statements in any order. While you are configuring the software, you can display all or portions of the candidate configuration, and you can insert or delete statements. Any changes you make affect only the candidate configuration, not the active configuration that is running on the router. For information about using the CLI and committing the current configuration, see the *JUNOS CLI User Guide*.

The configuration hierarchy logically groups related functions, which results in configuration statements that have a regular, consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy. For more information about the JUNOS hierarchy, see the *JUNOS Hierarchy and RFC Reference*.

At each level of the hierarchy, you can display a list of the statements available at that level, along with short descriptions of the statements' functions. To have the CLI complete the statement name if it is unambiguous or to provide a list of possible completions, you can type a partial statement name followed by a space or tab.

More than one user can edit a router's configuration simultaneously. All changes made by all users are visible to everyone editing the configuration. For more information, see the *JUNOS CLI User Guide*.

Activating a Configuration

To have a candidate configuration take effect, you commit the changes. At this point, 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.

The CLI always maintains a copy of previously committed versions of the software configuration. If you need to return to a previous configuration, you can do this from within the CLI. For more information, see the *JUNOS CLI User Guide*.

Managing Available Disk Space

A software installation or upgrade may fail if your router has a shortage of disk space. If a disk space error occurs, use one or more of the following options to complete the installation:

- Use the **request system storage cleanup** command to delete unnecessary files and increase storage space on the router.
- Specify the **unlink** option when you use the **request system software add** command to install the JUNOS software:
 - On the J-series platform, the **unlink** option removes the software package at the earliest opportunity to create enough disk space for the installation to finish.

- On the M-series and T-series platforms, the `unlink` option removes the software package after a successful upgrade.
- Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. The download program provides intelligent disk space management to enable installation.



NOTE: If you are upgrading the J-series router from a remote location, the installation program automatically checks for enough disk space for the process to finish.

For more information on the `request system storage cleanup` command and the `request system software add` command, see the *JUNOS System Basics and Services Command Reference*.

Using Software Monitoring Tools

The primary method of monitoring and troubleshooting the software, routing protocols, network connectivity, and the router hardware is to enter commands from the CLI. The CLI enables you to display information in the routing tables and routing protocol-specific data, and to check network connectivity using `ping` and `traceroute` commands.

The J-Web graphical user interface (GUI) is a Web-based alternative to using CLI commands to monitor, troubleshoot, and manage the router. For more information about J-Web, see “J-Web Package” on page 9.

The JUNOS software includes SNMP software, which allows you to manage routers. The SNMP software consists of an SNMP master agent and a MIB II agent, and supports MIB II SNMP version 1 traps and version 2 notifications, SNMP version 1 `Get` and `GetNext` requests, and version 2 `GetBulk` requests. For more information, see the *JUNOS Network Management Configuration Guide*.

The software also supports tracing and logging operations so that you can track events that occur in the router—both normal router operations and error conditions—and track the packets that are generated by or pass through the router. Logging operations use a `syslog`-like mechanism to record system-wide, high-level operations, such as interfaces going up or down and users logging in to or out of the router. Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions.

Router Security

Router security consists of three major elements: physical security of the router, operating system security, and security that can be effected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console. The inherent security of the JUNOS operating system also plays an important role in router security. The JUNOS software is extremely stable and robust. The JUNOS software also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

This section discusses some JUNOS software features available to improve router security:

- Router Access on page 19
- User Authentication on page 20
- Specifying Plain-Text Passwords on page 21
- Routing Protocol Security Features on page 22
- Firewall Filters on page 22
- Auditing for Security on page 22

Router Access

When you first install the JUNOS software, all remote access to the router is disabled, thereby ensuring that remote access is possible only if deliberately enabled by an authorized user. You can establish remote communication with a router in one of the following ways:

- Out-of-band management—Allows connection to the router through an interface dedicated to router management. Juniper Networks routing platforms support out-of-band management with a dedicated management Ethernet interface (`fxp0`), as well as EIA-232 console and auxiliary ports. The management Ethernet interface connects directly to the Routing Engine. No transit traffic is allowed through this interface, providing complete separation of customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the router.
- Inband management—Allows connection to the routers using the same interfaces through which customer traffic flows. While this approach is simple and requires no dedicated management resources, it has some disadvantages:
 - Management flows and transit traffic flows are mixed together. Any attack traffic that is mixed with the normal traffic can affect the communication with the router.
 - The links between router components might not be totally trustworthy, leading to the possibility of wiretapping and replay attacks.

For management access to the router, the standard ways to communicate with the router from a remote console are with Telnet and SSH. SSH provides secure encrypted communications and is therefore useful for inband router management. Telnet provides unencrypted, and therefore less secure, access to the router. For more information about router access, see the *JUNOS System Basics Configuration Guide*.

User Authentication

On a router, you can create local user login accounts to control who can log into the router and the access privileges they have. A password, either an SSH key or a Message Digest 5 (MD5) password, is associated with each login account. To define access privileges, you create login classes into which you group users with similar jobs or job functions. You use these classes to explicitly define what commands their users are and are not allowed to issue while logged in to the router.

The management of multiple routers by many different personnel can create a user account management problem. One solution is to use a central authentication service to simplify account management, creating and deleting user accounts only on a single, central server. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks (attacks in which someone uses a captured password to pose as a router administrator).

The JUNOS software supports two protocols for central authentication of users on multiple routers:

- Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).
- RADIUS, a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS. For more information about configuring user access, see the *JUNOS System Basics Configuration Guide*.

The JUNOS software also supports the following authentication methods:

- Internet Protocol Security (IPSec). IPSec architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). For more information about IPSec, see the *JUNOS Services Interfaces Configuration Guide*.
- MD5 authentication of MSDP peering sessions. This authentication provides protection against spoofed packets being introduced into a peering session. For more information about SNMPv3, see the *JUNOS Multicast Protocols Configuration Guide*.
- SNMPv3 authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules. For more information about SNMPv3, see the *JUNOS Network Management Configuration Guide*.

Specifying Plain-Text Passwords

The JUNOS software has special requirements when you create plain-text passwords on a routing platform. The default requirements for plain-text passwords are as follows:

- The password must be between 6 and 128 characters long.
- You can include uppercase letters, lowercase letters, numbers, punctuation marks, and any of the following special characters:

! @ # \$ % ^ & * , + = < > : ;

Control characters are not recommended.

- The password must contain at least one change of case or character class.

You can change the requirements for plain-text passwords. For more information, see the *JUNOS System Basics Configuration Guide*.

You can include the `plain-text-password` statement at the following hierarchy levels:

- [edit system diag-port-authentication]
- [edit system pic-console-authentication]
- [edit system root-authentication]
- [edit system login user *username* authentication]

Table 7 lists error messages that appear when you enter an invalid plain-text password.

Table 7: Plain-Text Password Error Messages

Error message	Problem with password
The minimum password length is <i>number</i> . (<i>number</i> is the default length configured.)	Too few characters; for example, abC.
Require additional changes of case, numbers or punctuation	Does not include the required changes of case, numbers or special characters; for example, abcdefg.
Passwords are not equal; aborting	Does not match the original password.

For more information about how to create plain-text passwords, see the *JUNOS System Basics Configuration Guide*.

Routing Protocol Security Features

The main task of a router is to forward user traffic toward its intended destination based on the information in the router's routing and forwarding tables. You can configure routing policies that define the flows of routing information through the network, controlling which routes the routing protocols place in the routing tables and which routes they advertise from the tables. You can also use routing policies to change specific route characteristics, change the BGP route flap-damping values, perform per-packet load balancing, and enable class of service (CoS).

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which can degrade the functionality of the router. To prevent such attacks, you must ensure that routers form routing protocol peering or neighboring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The JUNOS BGP, IS-IS, OSPF, RIP, and RSVP protocols support HMAC-MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

The JUNOS software supports the IPSec security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. The JUNOS software also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

Firewall Filters

Firewall filters allow you to control packets transiting the router to a network destination and packets destined for and sent by the router. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and the Routing Engine. Firewall filters provide a means of protecting your router from excessive traffic. Firewall filters that control local packets can also protect your router from external aggressions, such as DoS attacks.

To protect the Routing Engine, you can configure a firewall filter only on the router's loopback interface. Adding or modifying filters for each interface on the router is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine. For more information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

Auditing for Security

The JUNOS software logs significant events that occur on the router and within the network. Although logging itself does not increase security, you can use the system logs to monitor the effectiveness of your security policies and router configurations. You can also use the logs when reacting to a continued and deliberate attack as a means of identifying the source address, router, or port of the attacker's traffic. You can configure the logging of different levels of events, from only critical events to all events, including informational events. You can then inspect the contents of the system log files either in real time or later.

Debugging and troubleshooting are much easier when the timestamps in the system log files of all routers are synchronized, because events that span the network might be correlated with synchronous entries in multiple logs. The JUNOS software supports the Network Time Protocol (NTP), which you can enable on the router to synchronize the system clocks of routers and other networking equipment. By default, NTP operates in an unauthenticated mode. You can configure various types of authentication, including an HMAC-MD5 scheme. For more information about system logging, see the *JUNOS System Basics Configuration Guide* and the *JUNOS System Log Messages Reference*.

Chapter 3

Installing a Different JUNOS Software Version on a Router

This chapter describes how to install a different JUNOS software version on a routing platform—for example; to upgrade from JUNOS 7.6 to JUNOS 8.0.

For information about upgrading from JUNOS 5.x or later to 7.x or later, see the Knowledge Base Asset # 24602 on the Juniper Networks Support Web site at <http://www.juniper.net/support>.



NOTE: Downgrading by more than three releases may not be straightforward. In particular, if your routing platform is running JUNOS Release 7.5, you can downgrade directly to Release 7.2, but you cannot downgrade directly to Release 7.1. As a workaround, you can first downgrade to Release 7.2 and then downgrade to Release 7.1. See the release notes for each software release for details.

For information about JUNOS software media and packages, see “JUNOS Software Media and Packages” on page 1.

This chapter discusses the following topics:

- Confirming that Current Configuration Is Compatible with the Candidate Software on page 26
- Verifying PIC Combinations on page 26
- Determining Which JUNOS Software Version Is Running on page 27
- Upgrading All Software Packages on page 27
- Upgrading Individual Software Packages on page 31
- Installing the JUNOS Software on Routers with Redundant Routing Engines on page 32

Confirming that Current Configuration Is Compatible with the Candidate Software

When you upgrade or downgrade JUNOS software, we recommend that you include the `validate` option with the `request system software add` command to check that the candidate software is compatible with the current configuration. By default, when you add a package with a different release number, the validation check is done automatically. For more information about the `request system software add` command, see the *JUNOS System Basics and Services Command Reference*.

Verifying PIC Combinations

On Juniper Networks routing platforms, you can typically install any combination of Physical Interface Cards (PICs) on a single Enhanced Flexible PIC Concentrator (FPC) or in two PIC slots served by a single Layer 2/Layer 3 Packet Processing application-specific integrated circuit (ASIC).

Newer JUNOS services for some PICs can require significant Internet Processor ASIC memory, and some configuration rules limit certain combinations of PICs if they are installed on some platforms.

During software installation, the configuration checker in the installation program checks the router's PICs. If any configuration rules affect your PIC combinations, the installation process stops and displays a message similar to the following:

```
The combination of PICS in FPC slot 3 is not supported with this release
PIC slot 0 -
PIC slot 1 - 1x OC-12 ATM-II IQ
PIC slot 2 - 1x G/E IQ, 1000 BASE
PIC slot 3 - 1x Link Service (4)
If you continue the installation, one or more PICs on
FPC slot 3 might appear to be online but
cannot be enabled and cannot pass traffic with this release of JUNOS.
See the Release Notes for more information.
```

```
WARNING: This installation attempt will be aborted. If you
WARNING: wish to force the installation despite these warnings
WARNING: you may use the 'force' option on the command line.
pkg_add: package /var/tmp/jbundle-7.6R1.x-domestic-signed.tgz fails
requirements - not installed
```

The configuration checker has the following limitations:

- If a PIC is offline when you upgrade the router with new software, the configuration checker cannot detect PIC combinations affected by configuration rules and cannot warn about them.
- If you specify the `force` option when you upgrade the JUNOS software, the configuration checker warns about the affected PIC combination and the software installation continues. However, after rebooting, one or more PICs might fail to initialize.
- The configuration checker looks for combinations of three affected PICs. If an Enhanced FPC contains four affected PICs, the script generates multiple warnings.

If you install a PIC into a router already running JUNOS software, you can identify the presence of affected PIC combinations from messages in the system logging (syslog) file:

```
Feb 6 17:57:40 CE1 feb BCHIP 0: uCode overflow - needs 129 inst space to
load b3_atm2_LSI_decode for stream 12
Feb 6 17:57:41 CE1 chassisd[2314]: CHASSISD_IFDEV_DETACH_PIC:
ifdev_detach_pic(0/3)
Feb 6 17:57:41 CE1 feb BCHIP 0: binding b3_atm2_LSI_decode to stream 12
failed
Feb 6 17:57:41 CE1 feb PFE: can not bind B3 ucode prog b3_atm2_LSI_decode to
FPC 0: stream 12
```

For more information about checking for unsupported PIC combinations, see the corresponding PIC guide for your router, the *JUNOS Release Notes*, and *Technical Support Bulletin PSN-2004-12-002, PIC Combination Notes Summary* on the Juniper Networks Support Web site at <http://www.juniper.net/support/>.

Determining Which JUNOS Software Version Is Running

To determine which packages are running on the router and to get information about these packages, use the `show version` command at the top level of the command-line interface (CLI).

Upgrading All Software Packages

To upgrade all software packages, follow these steps:

1. Connect to the router console port using an out-of-band connection.
2. Copy stored files on the router to another file system. The upgrade process using the `jinstall` package removes stored files, except `juniper.conf` and SSH files on the router.
3. Download the `jinstall` software package from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. Choose the Canada and U.S., Worldwide, or JUNOS-FIPS edition. Place the package on the local server.

To download the software packages, you must have a service contract and an access account. If you do not have an access account, complete the registration form at the Juniper Networks Web site:
<https://www.juniper.net/registration/Register.jsp>.



NOTE: We recommend that you upgrade all software packages using an out-of-band connection from the console, because in-band connections are lost during the upgrade process.

4. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk, and the `/altroot` and `/altconfig` file systems are on the router's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.

5. Copy the `jinstall` package to the router. We recommend that you copy it to the `/var/tmp` directory, which is on the hard disk and is a large file system.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/  
filename /var/tmp/filename
```

6. Install the new software package, as shown below, where *package-name* is the full URL to the file. *release-number* is the major software release number; for example, 8.0R1. For more information about the `request system software add validate` command, see the *JUNOS System Basics and Services Command Reference*.

```
user@host> request system software add  
/var/tmp/jinstall-7.x-jinstall-package-name-signed.tgz  
Checking compatibility with configuration Initializing...  
Using jbase-8.x-package-name  
Using /var/tmp/jinstall-8.x-package-name.signed.tgz  
Verified jinstall-8.x-package-name.tgz signed by  
PackageDevelopment_0 Using  
/var/validate/tmp/jinstall-signed/jinstall-8.x-package-name.tgz  
Using /var/validate/tmp/jinstall/jbundle-8.x-package-name.tgz  
Checking jbundle requirements on /  
Using /var/validate/tmp/jbundle/jbase-8.x-package-name.tgz  
Using /var/validate/tmp/jbundle/jkernel-8.x-package-name.tgz  
Using /var/validate/tmp/jbundle/jcrypto-8.x-package-name.tgz  
Using /var/validate/tmp/jbundle/jpfe-8.x-package-name.tgz  
Using /var/validate/tmp/jbundle/jdocs-8.x-package-name.tgz  
Using /var/validate/tmp/jbundle/jroute-8.x-package-name.tgz  
Validating against /config/juniper.conf.gz  
mgd: commit complete  
Validation succeeded  
Installing package  
'/var/tmp/jinstall-8.x-package-name-signed.tgz' ...  
Verified jinstall-8.x-package-name-signed.tgz signed by  
PackageDevelopment_0  
Pre-checking requirements for jinstall...  
Auto-deleting old jinstall...  
Deleting saved config files...  
Deleting bootstrap installer...  
Adding jinstall...
```

```

WARNING: This package will load JUNOS 8.x software.
WARNING: It will save JUNOS configuration files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. It will attempt to preserve dumps
WARNING: and log files, but this can not be guaranteed. This is the
WARNING: pre-installation stage and all the software is loaded when
WARNING: you reboot the system.
Saving the config files...
Installing the bootstrap installer...

```

```

WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY.
WARNING: Use the 'request system reboot' command when software
WARNING: installation is complete. To abort the installation, do not reboot
WARNING: your system, instead use the 'request system software delete
WARNING: jinstall' command as soon as this operation completes.

```

```

Saving package file in
/var/sw/pkg/jinstall-8.x-package-name-signed.tgz...
Saving state for rollback...

```

7. Reboot the router to start the new software:

```

user@host> request system reboot
Reboot the system? [yes,no] (no) yes
Shutdown NOW!
Reboot consistency check bypassed - jinstall 8.xR1.12 will complete
installation upon reboot

*** FINAL System shutdown message from user@host-re0 ***
System going down IMMEDIATELY

```



NOTE: You must reboot to load the JUNOS software. To reboot, issue the `request system reboot` command when you are finished installing the software.

- To abort the installation, do not reboot your system; instead, finish the installation, then issue the `request system software delete jinstall` command. This is your last chance to stop the installation.
 - If JUNOS software doesn't install properly, you must install from the removable media. See "Reinstalling the JUNOS Software From Removable Media" on page 39.
-

All the software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not routing traffic.

8. Log in and verify the version of software running after the router reboots. Issue the `show version` command.

9. Add the optional `jweb` package using the `request system software add` command if you have already downloaded and copied it to the `/var/temp` directory. For more information about the `jweb` package, see “J-Web Package” on page 9.
10. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software.

The `request system snapshot` command causes the root file system to be backed up to `/altroot`, and `/config` to be backed up to `/altconfig`. The root and `/config` file systems are on the router’s flash disk, and the `/altroot` and `/altconfig` file systems are on the router’s hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and backup copy of the software are identical.

Upgrading Individual Software Packages

To upgrade an individual JUNOS software package, follow these steps:

1. Download the software package(s) you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. Choose either Canada and U.S. Version or Worldwide Version.

To download the software package(s), you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site: <https://www.juniper.net/registration/Register.jsp>.



NOTE: We recommend that you upgrade all individual software packages using an out-of-band connection from the console or `fxp0` interface, because in-band connections can be lost during the upgrade process.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk, and the `/altroot` and `/altconfig` file systems are on the router's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy and the backup copy of the software are identical.

3. If you are copying multiple software packages to the router, copy them to the `/var/tmp` directory on the hard disk.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/  
filename /var/tmp/filename
```

4. Add the new software package:

```
user@host> request system software add  
/var/tmp/package-name-signed.tgz  
Checking available free disk space...11200k available, 6076k suggested.
```

`package-name` is the full URL to the file.

The system might display the following message:

```
pkg_delete: couldn't entirely delete package
```

This message indicates that someone manually deleted or changed an item that was in a package. You do not need to take any action; the package is still properly deleted.

If you are upgrading more than one package at the same time, add `jbase` first. If you are using this procedure to upgrade all packages at once, add them in the following order:

```
user@host> request system software add /var/tmp/jbase-release-signed.tgz
user@host> request system software add
/var/tmp/jkernel-release-signed.tgz
user@host> request system software add /var/tmp/jpfe-release-signed.tgz
user@host> request system software add /var/tmp/jdocs-release-signed.tgz
user@host> request system software add /var/tmp/jweb-release-signed.tgz
user@host> request system software add
/var/tmp/jroute-release-signed.tgz
user@host> request system software add
/var/tmp/jcrypto-release-signed.tgz
```

5. Reboot the router to start the new software:

```
user@host> request system reboot
```

6. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software.

```
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk, and the `/altroot` and `/altconfig` file systems are on the router's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy, and backup copy of the software are identical.

Installing the JUNOS Software on Routers with Redundant Routing Engines

If the router has two Routing Engines, perform a JUNOS software installation on each Routing Engine separately to avoid disrupting network operation.

Install the new JUNOS software release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the newly installed Routing Engine to activate the new software. Finally, install the new software on the new backup Routing Engine.

To install a new version of JUNOS software on a router with redundant Routing Engines, follow these steps:

1. Log in to the master Routing Engine.
2. Enter the JUNOS software configuration mode:

```
{master}
user@host-re0> configure
```

3. Disable Routing Engine redundancy.

```
{master} [edit]
user@host-re0# delete chassis redundancy
```

4. Save the configuration change on both Routing Engines.

```
{master} [edit]
user@host-re0# commit synchronize and-quit
```

5. Log in to the backup Routing Engine.

```
{backup}
user@host-re0> request routing-engine login other routing-engine
```

6. Install the JUNOS software on the backup Routing Engine. See “Upgrading All Software Packages” on page 27.

```
{backup}
user@host-re1> request system software add
/var/tmp/jinstall-8.xxx.x-domestic-signed.tgz reboot
```

Notice that the host name changed, because you are now connected to the other Routing Engine.

7. The installation process reboots the router, activates the installation environment, and performs the installation without intervention. When the installation is complete, the backup Routing Engine reboots. During this time, you are logged out of the backup Routing Engine and returned to the master. You will not be able to log back in to the backup Routing Engine until the installation is complete. Use the `request routing-engine login other-routing-engine` command to periodically (every minute) determine whether the installation is complete.
8. Log out of the backup Routing Engine, then switchover to the other Routing Engine to change the role.

```
{backup}
user@host-re1> quit
{master}
user@host-re0> request chassis routing-engine master switch
{backup}
user@host-re0>
```

This command causes the backup Routing Engine, on which you just installed the software, become the master Routing Engine. The old master Routing Engine becomes the backup.

9. Install the new software version on the new backup Routing Engine which has become the master.

```
{backup}
user @host-re0> request system software add
/var/tmp/jinstall-8.xxx.x-domestic-signed.tgz reboot
```

10. When the Routing Engine reboots, you are logged out of the router. Log back in after a few minutes and restore the immediately proceeding redundancy configuration that existed before you deleted it in Step 3.

```
{backup}
user@host-re0> configure
[edit]
user@host-re0# rollback 1
```

11. Save the configuration change on both Routing Engines

```
[edit]
user@host-re0> commit synchronize and-quit
```

12. After you have installed the new software and are satisfied that the new software is successfully running, issue the `request system snapshot` command to back up the new software on both master and backup Routing Engines.

```
{master}
user@host-re0> request system snapshot
{master}
user@host-re0> request routing-engine login other routing-engine
{backup}
user@host-re1> request system snapshot
{backup}
user@host-re1> quit
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk, and the `/altroot` and `/altconfig` file systems are on the router's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy, and backup copy of the software are identical.

Chapter 4

Reinstalling the Software Using jinstall

If the JUNOS system software becomes damaged, you might want to reinstall it using `jinstall`. The `jinstall` package completely reinstalls the software. This package rebuilds the JUNOS file system only but retains configuration information from the previous version. Additionally, you cannot issue the `request system software rollback` command to return to the previously installed software after using a `jinstall` package. To return to the previously installed software, use the `jinstall` package for the release you want to return to.



NOTE: We recommend that you reinstall software packages out-of-band using the console, because in-band connections can be lost during the installation process.

The installation process removes stored files (except `juniper.conf` and SSH files) on the router, such as configuration templates and shell scripts. To preserve these files, copy them to another system before upgrading or downgrading the software.

To completely reinstall the software using `jinstall`, follow these steps:

1. Download the software packages you need from the Juniper Networks Support Web site, <http://www.juniper.net/support/>. Choose either the U.S. and Canada Version or the Worldwide Version.

To download the software packages, you must have a service contract and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks Web site:
<https://www.juniper.net/registration/Register.jsp>.

2. Back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

The root file system is backed up to `/altroot`, and `/config` is backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk, and the `/altroot` and `/altconfig` file systems are on the router's hard disk.



NOTE: After you issue the `request system snapshot` command, you cannot return to the previous version of the software, because the running copy, and backup copy of the software are identical.

- Copy the jinstall package to the /var/tmp directory on the hard disk.

```
user@host> file copy ftp://username:prompt@ftp.hostname.net/
filename /var/tmp/filename
```

- Add the jinstall package:

```
user@host> request system software add /var/tmp/
jinstall-8.x-package-name-signed.tgz
```

```
Installing package
'/var/tmp/jinstall-8.x-package-name-signed.tgz...
Verified jinstall-8.x-package-name-signed.tgz signed by PackageDevelopment_0
Adding jinstall...
```

```
WARNING: This package will load JUNOS 8.x software.
WARNING: It will save JUNOS configuration files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. It will attempt to preserve dumps
WARNING: and log files, but this can not be guaranteed. This is the
WARNING: pre-installation stage and all the software is loaded when
WARNING: you reboot the system.
```

```
Saving the config files...
Installing the bootstrap installer...
```

```
WARNING: A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY.
WARNING: Use the 'request system reboot' command when software installation
WARNING: is complete. To abort the installation, do not reboot your system,
WARNING: instead use the 'request system software delete jinstall'
WARNING: command as soon as this operation completes.
```

```
Saving package file in
/var/sw/pkg/jinstall-8.x-package-name-signed.tgz...
Saving state for rollback...
```

- If desired, add the optional jweb package. For more information, see “J-Web Package” on page 9.
- Reboot the router to load the JUNOS software:

```
user@host> request system reboot
Reboot the system? [yes,no] (no) yes
Shutdown NOW!
Reboot consistency check bypassed - jinstall 8.xR1.12 will complete
installation upon reboot

*** FINAL System shutdown message from user@host-re0 ***
System going down IMMEDIATELY
```



NOTE: You must reboot to load the JUNOS software. To reboot, issue the **request system reboot** command when you are finished installing the software.

To abort the installation, do not reboot your system; instead, issue the **request system software delete jinstall** command when you are done installing the software.

All the software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

7. Log in and verify the version of software running after the router reboots. Issue the **show log message** or **show version** command.
8. After you have upgraded or downgraded the software and are satisfied that the new software is successfully running, issue the **request system snapshot** command to back up the new software.

The **request system snapshot** command causes the root file system to be backed up to **/altroot**, and **/config** to be backed up to **/altconfig**. The root and **/config** file systems are on the router's flash disk, and the **/altroot** and **/altconfig** file systems are on the router's hard disk.



NOTE: After you issue the **request system snapshot** command, you cannot return to the previous version of the software, because the running copy, and backup copy of the software are identical.

Chapter 5

Reinstalling the JUNOS Software From Removable Media

When the router is shipped, a copy of the JUNOS software is provided on a removable media; a PC Card, which can be inserted in the router's drive or card slot.

If any of the software becomes damaged, you can reinstall it from the removable media.

This chapter discusses the following topics:

- Preparing to Reinstall the JUNOS Software on page 39
- Reinstalling the JUNOS Software on page 40
- Restoring the Saved Configuration on page 40

Preparing to Reinstall the JUNOS Software

Before you install the JUNOS software, you must do the following:

1. Have available the removable PC Card that shipped with the router. If you do not have a PC Card, contact customer support.
2. Use the `file copy` command to copy the existing configuration in the file `/config/juniper.conf` from the router to another system that is reachable through the router management interface (`fxp0`) or to removable media. Also, for extra safety, archive your backup configurations (the files named `/config/juniper.conf.n`, where `n` is a number from 0 through 9).

The install process completely overwrites the entire contents of the fixed storage media.

3. Copy any other stored files.

Reinstalling the JUNOS Software

To reinstall the JUNOS software, follow these steps:

1. Insert the removable medium into the router.



NOTE: You can store a configuration on install media such as PC Card.

2. Reboot the router. Do not power off the router if it is already on. Issue the `request system reboot` command from the command-line interface (CLI).
3. When the software asks the following question, type **y**:


```
WARNING: The installation will erase the contents of your disk. Do you wish
to continue (y/n)?
```
4. The router then copies the software from the removable medium onto your system, occasionally displaying status messages. Copying the software can take up to 10 minutes.
5. Remove the removable medium when prompted. The router then reboots from the boot device on which the software was just installed. When the reboot is complete, the router displays the login prompt.

Restoring the Saved Configuration

After you have reinstalled the software, you must copy the router's configuration files back to the router. (You also can configure the router from scratch, as described in "Configuring a Router for the First Time" on page 10.) However, before you can copy the configuration files, you must establish network connectivity.

To reconfigure the software, follow these steps:

1. Log in as `root`. There is no password.
2. Start the CLI:

```
root# cli
root@>
```

3. Enter configuration mode:

```
cli> configure
[edit]
root@#
```

4. Configure the name of the machine. If the name includes spaces, enclose the entire name in quotation marks (" ").

```
[edit]
root@# set system host-name host-name
```

5. Configure the machine's domain name:

```
[edit]
root@# set system domain-name domain-name
```

6. Configure the IP address and prefix length for the router's management Ethernet interface:

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

7. Configure the IP address of a default router. This system is called the backup router because it is used only while the routing protocol process is not running.

```
[edit]
root@# set system backup-router address
```

8. Configure the IP address of a Domain Name System (DNS) server:

```
[edit]
root@# set system name-server address
```

9. Set the root password, entering either a clear-text password that the system will encrypt, a password that is already encrypted, or an SSH public key string.

To enter a clear-text password, use the following command to set the root password:

```
[edit]
root@# set system root-authentication plain-text-password
New password: type password
Retype new password: retype password
```

To enter a password that is already encrypted, use the following command to set the root password:

```
[edit]
root@# set system root-authentication encrypted-password
encrypted-password
```

To enter an SSH public string, use the following command to set the root password:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

10. Commit the changes:

```
[edit]
root@# commit
```

After committing the configuration, you see the newly configured hostname after the username in the prompt—for example, `user@host#`.

11. Exit from configuration mode:

```
[edit]
root@host# exit
root@host>
```

12. To check that the router has network connectivity and to make sure you can reach the machine on which you saved your configuration files, issue a `ping` command to a system on the network:

```
root@> ping address
```

Use the address of the machine on which you copied the existing configuration in the file `/config/juniper.conf` and that is reachable through the router management interface (fxp0).

13. Copy the existing configuration and any backup configurations back to the router. Place the files in the `/config` directory. To copy the files, use the `file copy` command.
14. Load and activate the desired configuration:

```
root@> configure
[edit]
root@host# load merge /config/filename or load replace /config/filename
[edit]
root@# commit
```

15. Back up the JUNOS software. After you have installed the software on the router, committed the configuration, and are satisfied that the new configuration is successfully running, you should issue the `request system snapshot` command to back up the new software to the `/altconfig` file system. If you do not issue the `request system snapshot` command, the configuration on the alternate boot drive will be out of sync with the configuration on the primary boot drive.

The `request system snapshot` command causes the root file system to be backed up to `/altroot`, and `/config` to be backed up to `/altconfig`. The root and `/config` file systems are on the router's flash disk and the `/altroot` and `/altconfig` file systems are on the router's hard disk.

Index

A

access, router remotely 19
alternate boot device.....5
ASCII file, JUNOS software, configuring using8

B

boot devices5
boot sequence.....6

C

CLI
 JUNOS software, configuring using..... 8, 9
commit scripts
 JUNOS software, configuring using..... 8, 10
configuration
 activating..... 17
configuring
 methods for configuring JUNOS software8
conventions, documentationx
customer support
 contacting..... xv

D

disk space, available
 managing 17
documentation conventions.....x

F

FIPS *See* JUNOS-FIPS
firewall filters 22
flash disk, router storage media5

H

hard disk.....5
 router storage media5

I

icons defined, noticex
initial configuration
 JUNOS software 10

J

jbase individual software package 4
jbundle software package 4
 individual packages included 4
jcrypto individual software package 4
jdocs individual software package 4
jinstall software package..... 3
 individual packages included 4
 JUNOS software, reinstall using 35
jkernel individual software package 4
jpfe individual software package 4
jroute individual software package 4
J-series install bundle..... 4
JUNOS software..... 10
 downgrading more than three releases 25
 installation
 current configuration, confirming 26
 PIC combinations, verifying 26
 methods for configuring 8
 ASCII file 8
 CLI 8, 9
 commit scripts 8, 10
 JUNOScript API 8, 9
 J-Web GUI 8, 9
 NETCONF API 8, 10
 monitoring tools 18
 packages
 digital signatures 4
 jbundle (software bundle)..... 4
 jinstall (install package)..... 3
 junos-jseries 4
 MD5 checksum 5
 naming conventions 3
 SHA-1 checksum 4
 upgrading all 27
 passwords, plain-text, requirements 21
 reconfiguring 40
 redundant Routing Engines, initial
 configuration 14
 reinstall using jinstall..... 35

reinstalling	6, 39	router security	19
using removable media	40	access	19
release naming conventions	3	firewall filters	22
release numbers	3	JUNOS software, security, default settings	16
security, default settings	16	routing protocol security features	22
software properties, configuring	17	system log messages	22
storage media	5	user authentication	20
version, displaying	27	routers	
versions	2	boot sequence	6
Canada and U.S.	2	initial configuration	10
JUNOS-FIPS	2	JUNOS software	
worldwide	2	initial configuration for redundant Routing	
JUNOScript API		Engines	14
JUNOS software, configuring using	8, 9	remote access, establishing	19
JUNOS-FIPS		security features	19
installation and configuration requirements	3	storage media	5
password requirements	2	flash disk	5
junos-jseries software package	4	hard disk	5
J-Web graphical user interface (GUI)		removable	5
JUNOS software, configuring using	8, 9	Routing Engines	
jweb individual software package	4	available disk space, managing	17
		redundant	
		JUNOS software, initial configuration	14
		storage media device names	5
		routing protocol security features	22
M			
MD5 (Message Digest 5) checksum	5	S	
monitoring tools for JUNOS software	18	security	
		router, features	19
N		SHA-1 (Secure Hash Algorithm) checksum	4
NETCONF API		software packages, upgrading all	27
JUNOS software, configuring using	8, 10	storage media	5
notice icons defined	x	support, technical	
		customer support, contacting	xv
		system log messages	22
P		T	
PIC combinations		technical support	
verifying during JUNOS software installation	26	customer support, contacting	xv
plain-text password		typefaces, documentation conventions	x
error messages	21		
requirements	21	U	
primary boot device	5	user authentication	
		methods	20
R		protocols for central authentication	20
reconfiguring JUNOS software	40	router security	20
redundant Routing Engines			
installing JUNOS software	32		
reinstalling JUNOS software	39		
release names	3		
remote access, router, establishing	19		
removable media			
reinstalling JUNOS software, using	40		
router storage	5		