J4350 and J6350 Services Router

Getting Started Guide

Release 8.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, California 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-016824-01, Revision 1

J4350 and J6350 Services Router Getting Started Guide, Release 8.1
Copyright © 2006, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Nidhi Bhargava, Michael Bushong, Maya Devi, Taffy Everts, Walter Goralski, Joshua Kim, Jerry Isaac, Archana Maheshwari, Hareesh Kumar Kozhippurath Narayana Panicker, Laura Phillips, Cheryl Potter, Frank Reade, Swapna Steiger, Selvakumar T. S., Alan Twhigg, and Keldyn West
Editing: Taffy Everts and Stella Hackell
Illustration: Faith Bradford Brown and Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
13 October 2006—Revision 1.

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

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

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

End User License Agreement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS

OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

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

10. **Taxes.** All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

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

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

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

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

,

Abbreviated Table of Contents

About This Guide xv

Part 1 J-series Overview

Chapter 1 Overview of J4350 and J6350 Services Routers 3

Chapter 2 System Overview 9

Chapter 3 Physical Interface Modules Overview 27

Chapter 4 Services Router User Interface Overview 49

Part 2 Installing a Services Router

Chapter 5 Preparing for Router Installation 71

Chapter 6 Installing and Connecting a Services Router 81

Chapter 7 Establishing Basic Connectivity 93

Chapter 8 Configuring Secure Web Access 115

Chapter 9 Configuring Autoinstallation 125

Chapter 10 Installing and Managing J-series Licenses 131

Part 3 Maintaining Services Router Hardware

Chapter 11 Replacing and Troubleshooting Hardware Components 143

Chapter 12 Contacting Customer Support and Returning Hardware 175

Part 4 **J-series Requirements and Specifications**

Chapter 13 **Network Cable Specifications and Connector Pinouts** 185

Chapter 14 **Safety and Regulatory Compliance Information** 201

Part 5 **Index**

Table of Contents

About This Guide xv

Objectives xv
Audience xvi
Document Conventions xvi
Related Juniper Networks Documentation xviii
Documentation Feedback xx
Requesting Support xx

Part 1 J-series Overview

Chapter 1 Overview of J4350 and J6350 Services Routers 3

J4350 Services Router Overview 4
J6350 Services Router Overview 4
J-series Software Features and Licenses 5

Chapter 2 System Overview 9

J4350 and J6350 Services Router Hardware Features 9
- Chassis 9
- Midplane 14
- Routing Engine 14
  - Boot Devices 15
- Front Panel 15
  - Physical Interface Modules (PIMs) 16
  - Power Button and POWER LED 17
  - STATUS LED 18
  - ALARM LED 18
  - HA LED 19
  - RESET CONFIG Button 19
  - Built-In Gigabit Ethernet Ports 19
  - Console Port 20
  - AUX Port 20
  - USB Port 20
- J4350 Power System 21
- J6350 Power System 21
- Cooling System 22

Software Overview 23
- Routing Engine and Packet Forwarding Engine 24

Kernel and Microkernel ... 24
JUNOS Software Processes ... 24
User Interfaces ... 25

Chapter 3 Physical Interface Modules Overview 27

PIM Terms ... 27
Field-Replaceable PIMs ... 29
Field-Replaceable PIM Summary ... 30
Gigabit Ethernet ePIMs ... 31
Dual-Port Serial PIM ... 34
Dual-Port T1 or E1 PIM ... 35
Dual-Port Channelized T1 or E1 PIM ... 36
T3 or E3 PIM ... 38
Dual-Port Fast Ethernet PIM ... 40
4-Port Fast Ethernet ePIM ... 41
4-Port ISDN BRI PIMs ... 42
ADSL PIM ... 44
G.SHDSL PIM ... 46

Chapter 4 Services Router User Interface Overview 49

User Interface Overview ... 49
J-Web Overview ... 49
CLI Overview ... 50
Comparison of Configuration Interfaces ... 50
Before You Begin ... 52
Using the J-Web Interface ... 52
Starting the J-Web Interface ... 53
J-Web Layout ... 53
J-Web Sessions ... 58
Using the Command-Line Interface ... 58
CLI Command Hierarchy ... 58
Starting the CLI ... 59
CLI Operational Mode ... 60
CLI Configuration Mode ... 61
CLI Basics ... 62
Editing Keystrokes ... 62
Command Completion ... 63
Online Help ... 63
Configuring the CLI Environment ... 65

Part 2 Installing a Services Router

Chapter 5 Preparing for Router Installation 71

General Site Guidelines ... 71
Rack Requirements ... 72

Rack Size and Strength 72
Connection to Building Structure 73
Router Environmental Tolerances 73
Fire Safety Requirements 73
Fire Suppression 74
Fire Suppression Equipment 74
Power Guidelines, Requirements, and Specifications 74
Site Electrical Wiring Guidelines 75
Signaling Limitations 75
Radio Frequency Interference 75
Electromagnetic Compatibility 75
Router Power Requirements 76
AC Power, Connection, and Power Cord Specifications 76
DC Power, Connection, and Power Cable Specifications 77
Network Cable Specifications 78
ISDN Provisioning 79
Site Preparation Checklist 79

Chapter 6 Installing and Connecting a Services Router 81

Before You Begin 81
Unpacking a J-series Services Router 82
Installing a J4350 and J6350 Services Router 83
Connecting Interface Cables to a Services Router 85
Chassis Grounding 86
Connecting Power 86
Connecting AC Power 86
Connecting DC Power 88
Powering a Services Router On and Off 90

Chapter 7 Establishing Basic Connectivity 93

Basic Connectivity Terms 93
Basic Connectivity Overview 94
Router Identification 95
Root Password 95
Time Zone and System Time 95
Network Settings 96
Default Gateway 96
Backup Router 96
Loopback Address 96
Built–In Ethernet Interface Address 97
Management Access 97
Before You Begin 98
Connecting to a Services Router 99
Connecting to the J-Web Interface 99
Connecting to the CLI Locally 101
Connecting to the CLI Remotely 103
Configuring the Modem at the Router End 103
Connecting the Modem to the Console Port 104
Connecting to the CLI at the User End 104
Configuring Basic Settings with J-Web Quick Configuration 105

Configuring Basic Settings with a Configuration Editor....108
Verifying Basic Connectivity....113
Displaying Basic Connectivity Configurations....113

Chapter 8 Configuring Secure Web Access 115

Secure Web Access Terms....115
Secure Web Access Overview....116
Before You Begin....117
Generating SSL Certificates....117
Configuring Secure Web Access with Quick Configuration....117
Configuring Secure Web Access with a Configuration Editor....121
Verifying Secure Web Access....122
Displaying an SSL Certificate Configuration....122
Displaying a Secure Access Configuration....123

Chapter 9 Configuring Autoinstallation 125

Autoinstallation Terms....125
Autoinstallation Overview....126
Autoinstallation Interfaces....126
Autoinstallation Process on Services Router....126
Automatic Configuration of a New Services Router....127
Before You Begin....127
Configuring Autoinstallation with a Configuration Editor....128
Verifying Autoinstallation....129
Verifying Autoinstallation Status....129

Chapter 10 Installing and Managing J-series Licenses 131

J-series License Overview....131
Software Feature Licenses....131
License Key Components....132
Before You Begin....132
Managing J-series Licenses with the J-Web Interface....133
Adding New Licenses with the J-Web Interface....134
Deleting Licenses with the J-Web Interface....135
Displaying License Keys with the J-Web Interface....135
Downloading Licenses with the J-Web Interface....135
Managing J-series Licenses with the CLI....136
Adding New Licenses with the CLI....136
Deleting a License with the CLI....136
Saving License Keys with the CLI....137
Verifying J-series License Management....137
Displaying Installed Licenses....137
Displaying License Usage....138
Displaying Installed License Keys....139

Part 3 Maintaining Services Router Hardware

Chapter 11 Replacing and Troubleshooting Hardware Components 143

Replacing Hardware Components....143
- Tools and Parts Required....144
- Replacing the Console Port Cable....144
- Replacing a PIM....144
  - Removing a PIM....145
  - Installing a PIM....146
- Replacing PIM Cables....147
  - Removing a PIM Cable....148
  - Installing a PIM Cable....148
- Replacing the Compact Flash Disk....149
- Removing and Installing the USB Storage Device....153
  - Removing the USB Storage Device....154
  - Installing the USB Storage Device....155
- Removing and Installing DRAM Modules....155
  - Removing a DRAM Module....156
  - Installing a DRAM Module....157
- Replacing Power System Components....158
  - Replacing an AC Power Supply Cord....159
  - Removing an AC Power Supply from a J6350 Router....160
  - Installing an AC Power Supply in a J6350 Router....161
  - Replacing a DC Power Supply Cable....162
  - Removing a DC Power Supply from a J6350 Router....163
  - Installing a DC Power Supply in a J6350 Router....165
- Removing and Installing a Crypto Accelerator Module....167
  - Removing the Crypto Accelerator Module....167
  - Installing a Crypto Accelerator Module....169
- Replacing an Air Filter....170

Troubleshooting Hardware Components....171
- Chassis Alarm Conditions....171
- Contacting the Juniper Networks Technical Assistance Center....173

Chapter 12 Contacting Customer Support and Returning Hardware 175

Locating Component Serial Numbers....175
- PIM Serial Number Label....177
- J6350 Power Supply Serial Number Labels....177

Contacting Customer Support....178
- Information You Might Need to Supply to JTAC....178

Return Procedure....178

Packing a Router or Component for Shipment....179
- Tools and Parts Required....179
- Packing the Services Router for Shipment....180
- Packing Components for Shipment....181

Part 4 J-series Requirements and Specifications

Chapter 13 Network Cable Specifications and Connector Pinouts 185

Serial PIM Cable Specifications 185
RS-232 DTE Cable Pinout 186
RS-232 DCE Cable Pinout 187
RS-422/449 (EIA-449) DTE Cable Pinout 187
RS-422/449 (EIA-449) DCE Cable Pinout 188
EIA-530A DTE Cable Pinout 189
EIA-530A DCE Cable Pinout 190
V.35 DTE Cable Pinout 191
V.35 DCE Cable Pinout 192
X.21 DTE Cable Pinout 193
X.21 DCE Cable Pinout 193
RJ-45 Connector Pinout for Fast Ethernet Ports 194
RJ-45 Connector Pinout for Gigabit Ethernet Ports 195
Console Port Pinouts 195
E1 and T1 RJ-48 Cable Pinouts 196
E3 and T3 BNC Connector Pinout 198
ADSL and G.SHDSL RJ-11 Connector Pinout 199
ISDN RJ-45 Connector Pinout 199

Chapter 14 Safety and Regulatory Compliance Information 201

Definition of Safety Warning Levels 201
Safety Guidelines and Warnings 203
General Safety Guidelines and Warnings 203
Qualified Personnel Warning 204
Preventing Electrostatic Discharge Damage 205
Electrical Safety Guidelines and Warnings 206
General Electrical Safety Guidelines 207
AC Power Electrical Safety Guidelines 208
Power Cable Warning (Japanese) 208
DC Power Electrical Safety Guidelines 209
Power Sources for Redundant Power Supplies 209
DC Power Disconnection Warning 210
DC Power Grounding Requirements and Warning 211
DC Power Wiring Sequence Warning 212
DC Power Wiring Terminations Warning 213
Grounded Equipment Warning 214
Warning Statement for Norway and Sweden 215
In Case of Electrical Accident 215
Multiple Power Supplies Disconnection Warning 215
Power Disconnection Warning 217
TN Power Warning 218
Telecommunication Line Cord Warning 219
Installation Safety Guidelines and Warnings 221
Chassis Lifting Guidelines 221

Installation Instructions Warning 221
Rack-Mounting Requirements and Warnings 222
Ramp Warning 226
Laser and LED Safety Guidelines and Warnings 227
General Laser Safety Guidelines 227
Class 1 Laser Product Warning 227
Class 1 LED Product Warning 228
Laser Beam Warning 229
Radiation from Open Port Apertures Warning 230
Maintenance and Operational Safety Guidelines and Warnings 231
Battery Handling Warning 232
Jewelry Removal Warning 233
Lightning Activity Warning 235
Operating Temperature Warning 236
Product Disposal Warning 238
Agency Approvals 240
Compliance Statements for Environmental Requirements 241
Lithium Battery 241
Compliance Statements for EMC Requirements 241
Canada 241
European Community 243
Japan 244
Taiwan 244
United States 244
FCC Part 15 Statement 245
FCC Part 68 Statement 245
Product Reclamation and Recycling Program 246

Part 5 Index

Index 249

About This Guide

This preface provides the following guidelines for using the *J4350 and J6350 Services Router Getting Started Guide*:

- Objectives on page xv
- Audience on page xvi
- Document Conventions on page xvi
- Related Juniper Networks Documentation on page xviii
- Documentation Feedback on page xx
- Requesting Support on page xx

Objectives

This guide contains an overview, basic instructions, and specifications for J4350 and J6350 Services Routers. It explains how to prepare your site for installation, unpack and install a Services Router and its components, power on the router, install licenses, and establish basic connectivity.

NOTE: This guide documents Release 8.1 of the JUNOS software. For additional information about J-series Services Routers—either corrections to or omissions from this guide—see the *J-series Services Router Release Notes* at http://www.juniper.net.

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

Table 1: Capabilities of J-series Interfaces

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

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

Although the *J-Web Interface User Guide* provides a useful overview of the J-Web interface, it contains only a subset of J-Web information. We recommend that J-series users consult the J-series Services Router guides, instead.

Audience

This guide is designed for anyone who installs and sets up a J-series Services Router or prepares a site for Services Router installation. The guide is intended for the following audiences:

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

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

Document Conventions

Table 2 defines the notice icons used in this guide.

Table 2: Notice Icons

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

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

Table 3: Text and Syntax Conventions

Convention	Description	Examples
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width typeface`	Represents output that appears on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic typeface	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic sans serif typeface	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Sans serif typeface	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast | multicast (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		

Convention	Description	Examples
Bold typeface	Represents J-Web graphical user interface (GUI) items you click or select.	■ In the Logical Interfaces box, select **All Interfaces**. ■ To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols > Ospf**.

Related Juniper Networks Documentation

J-series Services Routers are documented in multiple guides. Although the J-series guides provide instructions for configuring and managing a Services Router with the JUNOS CLI, they are not a comprehensive JUNOS software resource. For complete documentation of the statements and commands described in J-series guides, see the JUNOS software manuals listed in Table 4.

Table 4: J-series Guides and Related JUNOS Software Publications

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
Getting Started Guide for Your Router	
"Services Router User Interface Overview" "Establishing Basic Connectivity" "Configuring Autoinstallation"	■ *JUNOS CLI User Guide* ■ *JUNOS System Basics Configuration Guide*
J-series Services Router Basic LAN and WAN Access Configuration Guide	
"Using Services Router Configuration Tools"	■ *JUNOS CLI User Guide* ■ *JUNOS System Basics Configuration Guide*
"Interfaces Overview" "Configuring DS1, DS3, Ethernet, and Serial Interfaces" "Configuring Digital Subscriber Line Interfaces "Configuring Point-to-Point Protocol over Ethernet" "Configuring ISDN"	■ *JUNOS Network Interfaces Configuration Guide* ■ *JUNOS Interfaces Command Reference*
"Configuring Link Services Interfaces"	■ *JUNOS Services Interfaces Configuration Guide* ■ *JUNOS System Basics and Services Command Reference*

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

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

Documentation Feedback

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

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

Requesting Support

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

Part 1
J-series Overview

- Overview of J4350 and J6350 Services Routers on page 3
- System Overview on page 9
- Physical Interface Modules Overview on page 27
- Services Router User Interface Overview on page 49

Chapter 1

Overview of J4350 and J6350 Services Routers

J-series Services Routers provide stable, reliable, and efficient IP routing, WAN and LAN connectivity, and management services for small to medium-sized enterprise networks. Services Routers typically connect small, branch, or regional offices to a central site router, and link Internet service provider (ISP) networks.

All J-series Services Routers run the JUNOS Internet software, which offers many advanced routing and security services. For more information about software features, see "J-series Software Features and Licenses" on page 5. A single, common JUNOS code base simplifies deployment, patches, and software upgrades.

You can use two user interfaces to monitor, configure, troubleshoot, and manage a Services Router:

- J-Web Web–based interface—Allows you to manage your Services Router without using the command-line interface (CLI). The J-Web interface provides access to all JUNOS functionality and features. The J-Web interface also provides Quick Configuration wizards to simplify operations and minimize the risk of operator error.

- JUNOS command–line interface—The JUNOS CLI is a Juniper Networks command shell that runs on top of a UNIX-based operating system kernel. The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI provides command help and command completion.

For an introduction to the J-Web and CLI interfaces, see "Services Router User Interface Overview" on page 49. For additional information about CLI commands, see the *JUNOS CLI User Guide*.

This chapter contains the following topics:

- J4350 Services Router Overview on page 4

- J6350 Services Router Overview on page 4

- J-series Software Features and Licenses on page 5

J4350 Services Router Overview

The J4350 Services Router is designed primarily for regional or branch offices. It has a chassis that is 2 U (rack units) in size with a nonredundant AC or DC power supply, and a Universal Serial Bus (USB) port for external storage.

J4350 routers ordered with the optional Crypto Accelerator card come standard with 1 GB of memory, while those ordered without the Crypto Accelerator card come standard with 256 MB of memory. J4350 routers can contain between 256 MB and 2 GB of memory. For instructions on adding memory, see “Removing and Installing DRAM Modules” on page 155.

Each J4350 chassis contains four built-in Gigabit Ethernet ports with link speeds of 10/100/1000 Mbps over a copper interface, and six slots for field-replaceable Physical Interface Modules (PIMs). Two of the six slots (slots 3 and 6) support high-speed interfaces (ePIMs).

The J4350 Services Router supports the following field-replaceable Physical Interface Modules (PIMs):

- SFP Gigabit Ethernet ePIM (1 port)
- Copper Gigabit Ethernet ePIM (1 port)
- ADSL 2/2 + Annex A PIM (1 port)
- ADSL 2/2 + Annex B PIM (1 port)
- Dual-Port E1 PIM
- E3 PIM (1 port)
- DS3 (T3) PIM (1 port)
- Dual-Port Fast Ethernet PIM
- 4–port Fast Ethernet ePIM
- G.SHDSL PIM (2 ports)
- 4-port ISDN BRI S/T or U PIM
- Dual-Port Serial PIM
- Dual-Port T1 PIM

J6350 Services Router Overview

The J6350 Services Router is designed primarily for regional or central offices. It has a chassis that is 2 U (rack units) in size with an optional redundant AC or DC power supply, up to 2 GB of memory, and two Universal

Serial Bus (USB) ports for external storage. The J6350 Services Router is a higher-performance system than the J4350 Services Router.

J6350 routers come standard with 1 GB of memory and can contain between 256 MB to 2 GB of memory. For instructions on adding memory, see "Removing and Installing DRAM Modules" on page 155.

Each J6350 chassis contains four built-in Gigabit Ethernet ports with link speeds of 10/100/1000 Mbps over a copper interface, and six slots for field-replaceable Physical Interface Modules (PIMs). Four of the six slots (slots 2, 3, 5, and 6) support high-speed interfaces (ePIMs).

The J6350 Services Router supports the following field-replaceable PIMs:

- SFP Gigabit Ethernet ePIM (1 port)
- Copper Gigabit Ethernet ePIM (1 port)
- ADSL Annex A PIM (1 port)
- ADSL Annex B PIM (1 port)
- Dual-Port E1 PIM
- E3 PIM (1 port)
- DS3 (T3) PIM (1 port)
- Dual-Port Fast Ethernet PIM
- 4–port Fast Ethernet ePIM
- G.SHDSL PIM (2 ports)
- 4-port ISDN BRI S/T or U PIM
- Dual-Port Serial PIM
- Dual-Port T1 PIM

J-series Software Features and Licenses

J-series Services Routers provide the software features listed in Table 5. You must purchase a separate software license to obtain some software features. For more information about licenses, see "Installing and Managing J-series Licenses" on page 131.

Table 5: Summary of J-series Features and License Requirements

Feature Category	J-series Feature	Separate License
Internet Protocols	IPv4	
	IPv6 routing and forwarding	
Routing and Multicast	Open Shortest Path First (OSPF)	
	Border Gateway Protocol (BGP)	License required for advanced BGP (route reflectors)
	Routing Information Protocol version 1 (RIPv1) and RIPv2	
	Static routes	
	Intermediate System-to-Intermediate System (IS-IS)	
	Connectionless Network Services (CLNS): ■ End system-to-Intermediate system (ES-IS) protocol ■ IS-IS extensions ■ BGP extensions ■ Static routes	
	Multiprotocol Label Switching (MPLS): ■ Layer 2 and Layer 3 virtual private networks (VPNs) ■ VPN routing and forwarding (VRF) table labels ■ Traffic engineering protocols: ▪ Label Distribution Protocol (LDP) ▪ Resource Reservation Protocol (RSVP)	
	Multicast: ■ Internet Group Management Protocol version 3 (IGMPv3) ■ Protocol Independent Multicast (PIM) ■ Distance Vector Multicast Routing Protocol (DVMRP) ■ Single-source multicast	
IP Address Management	Static addresses	
	Dynamic Host Configuration Protocol (DHCP)	

Table 5: Summary of J-series Features and License Requirements (continued)

Feature Category	J-series Feature	Separate License
Encapsulation	Ethernet: ■ Media access control (MAC) encapsulation ■ 802.1p tagging ■ Point-to-Point Protocol over Ethernet (PPPoE) ■ Asynchronous Transfer Mode (ATM) for asymmetric digital subscriber line (ADSL) or symmetric high-speed digital subscriber line (SHDSL) ■ Circuit cross-connect (CCC) ■ Translational cross-connect (TCC)	
	Synchronous Point-to-Point Protocol (PPP)	
	Frame Relay	
	High-level Data Link Control (HDLC)	
	Serial encapsulation over RS-232, RS-449, X.21, V.35, and EIA-530 connections	
	802.1Q filtering and forwarding	
	Multilink Frame Relay	
	Multilink PPP	
	Data link switching (DLSw)	License required
Traffic Management	Policing and shaping	
	Class-based queuing with prioritization	
	Weighted random early detection (WRED)	
	Queuing by virtual LAN (VLAN), data link connection identifier (DLCI), interface, or bundle	
Security	Common Criteria	
	Network attack detection	
	Denial-of-service (DoS) and distributed DoS protection	
	Generic routing encapsulation (GRE), IP-over-IP, and IP Security (IPSec) tunnels	
	Advanced Encryption Standard (AES) 128-, 192-, and 256-bit.	
	56-bit Data Encryption Standard (DES) and 168-bit 3DES encryption	
	MD5 and Secure Hash Algorithm (SHA-1) authentication	
	Replay attack prevention	
	Stateful firewall packet filters	
	Network Address Translation (NAT)	
Voice Support	Compressed Real-Time Transport Protocol (CRTP)	

Table 5: Summary of J-series Features and License Requirements (continued)

Feature Category	J-series Feature	Separate License
High Availability	Virtual Router Redundancy Protocol (VRRP)	
	Graceful restart according to IETF standards	
	Redundant interfaces	
System Management	JUNOScope network manager	
	J-Web browser interface—for Services Router configuration and management	
	JUNOScript XML application programming interface (API)	
	JUNOS command-line interface (CLI)—for Services Router configuration and management through the console, Telnet, or SSH	
	Simple Network Management Protocol version 1 (SNMPv1) and SNMPv2	
Traffic Analysis	J-Flow flow monitoring and accounting	License required for J-Flow
	Packet capture (PCAP)	
	Real-time performance monitoring (RPM)	
Activity Logging and Monitoring	System log	
	J-Web event viewer	
	Traceroute	
Administration	Supports the following external administrator databases: ■ RADIUS ■ TACACS +	
	Autoinstallation	
	Configuration rollback	
	Button-operated configuration rescue (CONFIG)	
	Confirmation of configuration changes	
	Software upgrades	
	Supports the following features for automating network operations and troubleshooting: ■ Commit scripts ■ Operation scripts ■ Event policies	

Chapter 2

System Overview

The J4350 and J6350 Services Routers have chassis that are similar but with important differences. J4350 routers have nonredundant power supplies, six slots, including two enhanced (high-speed) slots, and an optional Crypto Accelerator Module. J6350 routers have redundant power supplies, six slots, including four enhanced (high-speed) slots, and a standard Crypto Accelerator Module.

All J-series routers run the JUNOS Internet software.

This chapter contains the following topics:

- J4350 and J6350 Services Router Hardware Features on page 9
- Software Overview on page 23

J4350 and J6350 Services Router Hardware Features

This section contains the following topics:

- Chassis on page 9
- Midplane on page 14
- Routing Engine on page 14
- Front Panel on page 15
- J4350 Power System on page 21
- J6350 Power System on page 21
- Cooling System on page 22

Chassis

The Services Router chassis is a rigid sheet metal structure that houses all the other router components (see Figure 1 through Figure 6). The chassis can be installed in many types of racks or cabinets. For information about acceptable rack types, see “Rack Requirements” on page 72.

In addition to the features described in subsequent sections, the chassis includes the following features:

- One pair of metal brackets can be mounted at the front or center of the chassis. Use the brackets for mounting the chassis in a rack or cabinet.
- Two protective earthing terminals, PEM nuts at the rear of the chassis.
- One electrostatic discharge (ESD) point, a banana plug receptacle at the front of the chassis.

CAUTION: Before removing or installing components of a functioning router, attach an ESD strap to an ESD point and place the other end of the strap around your bare wrist. Failure to use an ESD strap could result in damage to the router.

The router must be connected to earth ground during normal operation. The protective earthing terminals on the rear of the chassis are provided to connect the router to ground (see Figure 3). Additional grounding is provided to an AC-powered router when you plug its power supply into a grounded AC power receptacle.

For additional safety information, see “Safety and Regulatory Compliance Information” on page 201.

Figure 1: Front of J4350 and J6350 Chassis

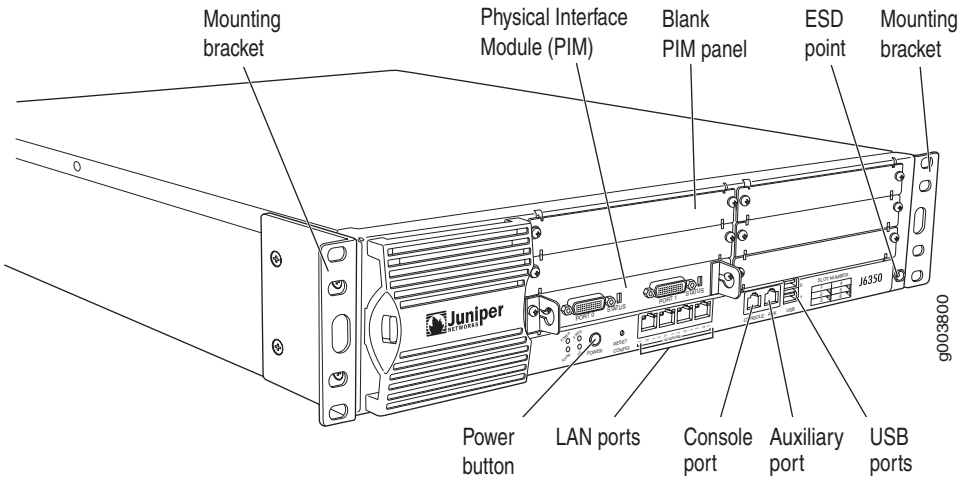
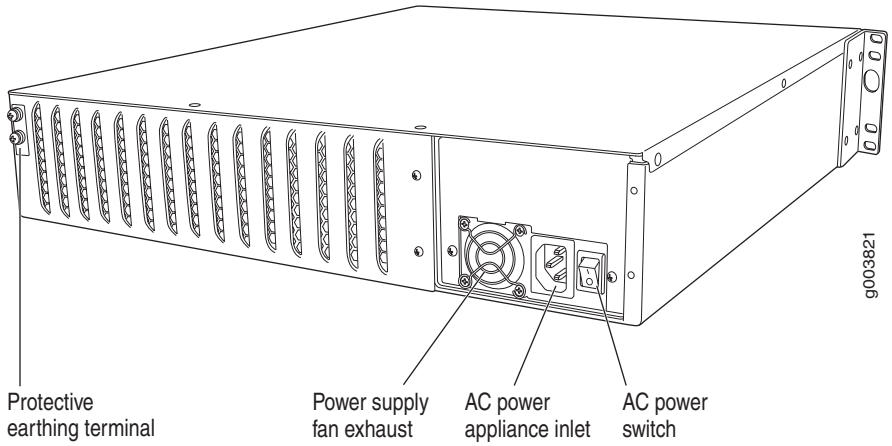


Figure 2: Rear of J4350 AC-Powered Chassis



NOTE: The J4350 AC-powered chassis has a power switch and does not include a power supply LED (unlike the J6350 AC-powered chassis).

Figure 3: Rear of J6350 AC-Powered Chassis

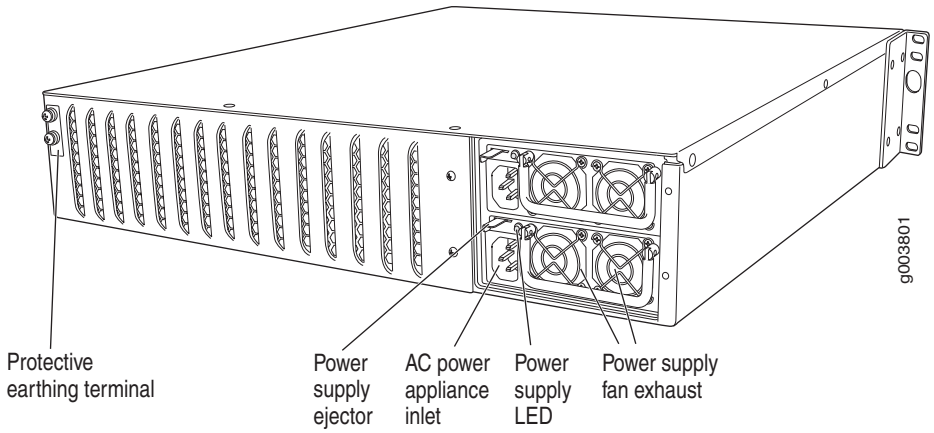


Figure 4: Rear of J4350 DC-Powered Chassis

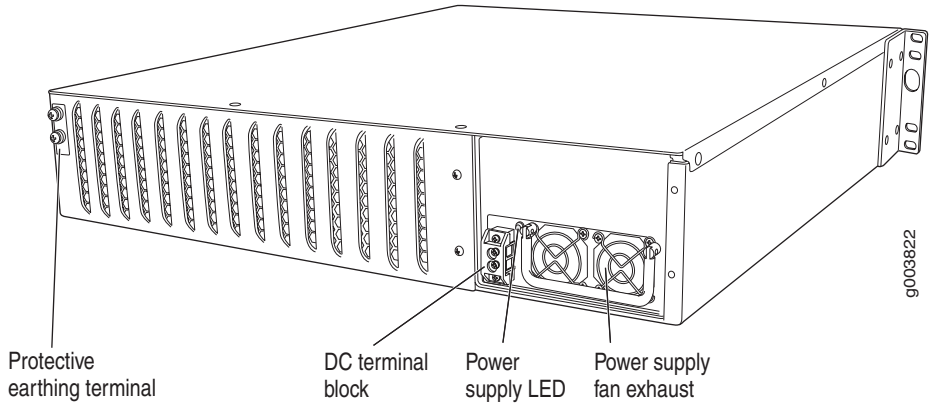


Figure 5: Rear of DC-Powered J6350 Chassis

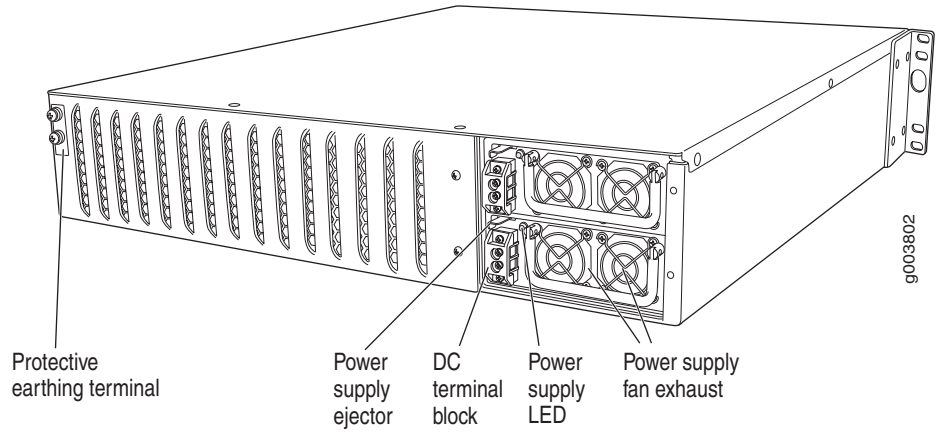


Figure 6: J4350 and J6350 Hardware Components

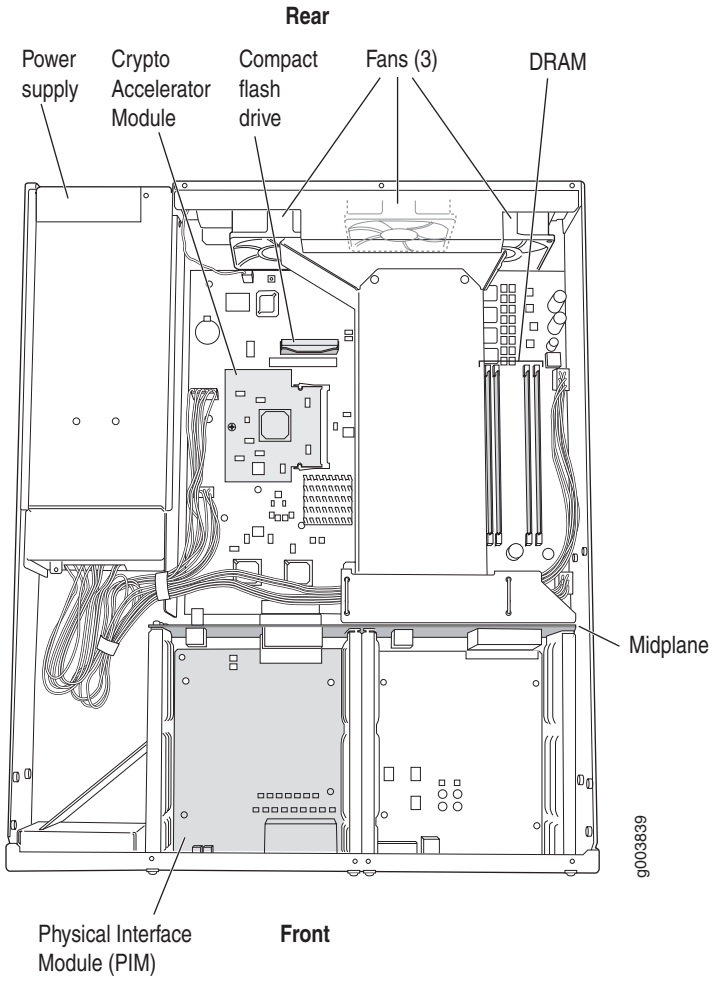


Table 6 summarizes the physical specifications for the router chassis.

Table 6: J4350 and J6350 Physical Specifications

Description	Value
Chassis dimensions	■ 3.44 in. (8.74 cm) high ■ 17.44 in. (44.3 cm) wide—19.44 in. (48.38 cm) wide with mounting brackets attached ■ 21.13 in. (53.67 cm) deep—plus 0.5 in. (1.27 cm) of hardware that protrudes from the chassis front
Router weight	■ J4350 Services Router: ▪ Minimum (no PIMs): 23 lb (10.4 kg) ▪ Maximum (six PIMs): 25.3 lb (11.5 kg) ■ J6350 router ▪ Minimum (no PIMs and one power supply): 25.5 lb (11.6 kg) ▪ Maximum (six PIMs and two power supplies): 30.7 lb (13.9 kg)

Midplane

The midplane is located in the center of the chassis and forms the rear of the PIM card cage (see Figure 6). You install the PIMs into the midplane from the front of the chassis. Data packets are transferred across the midplane from the PIM to the Routing Engine, and from the Routing Engine across the midplane to the destination PIM.

Routing Engine

The Routing Engine provides three main functions:

- Creates the packet forwarding switch fabric for the Services Router, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the router and controls the routing protocols that run on the router.
- Provides control and monitoring functions for the router, including controlling power and monitoring system status.

The Routing Engine consists of the following components:

- Processor—Creates the packet forwarding switch fabric for the router and runs JUNOS Internet software to maintain the router's routing tables and routing protocols.
- DRAM—Buffers incoming packets and provides storage for the routing and forwarding tables and for other Routing Engine processes.

To view the amount of DRAM installed on your router, issue the show chassis routing-engine command.

- EPROM—Stores the serial number of the Routing Engine.

  To view the serial number of the Routing Engine, issue either the show chassis routing-engine command or the show chassis hardware command.

- Crypto Accelerator Module—Processor card that enhances performance of cryptographic algorithms used in IP security (IPSec) services. The cryptographic algorithms supported include Advanced Encryption Standard (AES), Data Encryption Standard (DES), triple DES (3DES), Hashed Message Authentication Code-Message Digest 5 (HMAC-MD5), and HMAC-Secure Hash Algorithm 1 (SHA-1). The Crypto Module is a standard feature of J6350 Services Routers and an optional feature of J4350 Services Routers.

  To determine whether there is a Crypto Accelerator Module installed on your router, issue the show chassis hardware command.

- Compact flash drive—Provides primary storage for software images, configuration files, and microcode. J4350 and J6350 routers have an internal compact flash drive, located on the motherboard. For information about replacing the compact flash drive, see “Replacing the Compact Flash Disk” on page 149.

Boot Devices

The J4350 and J6350 Services Routers can boot from two devices:

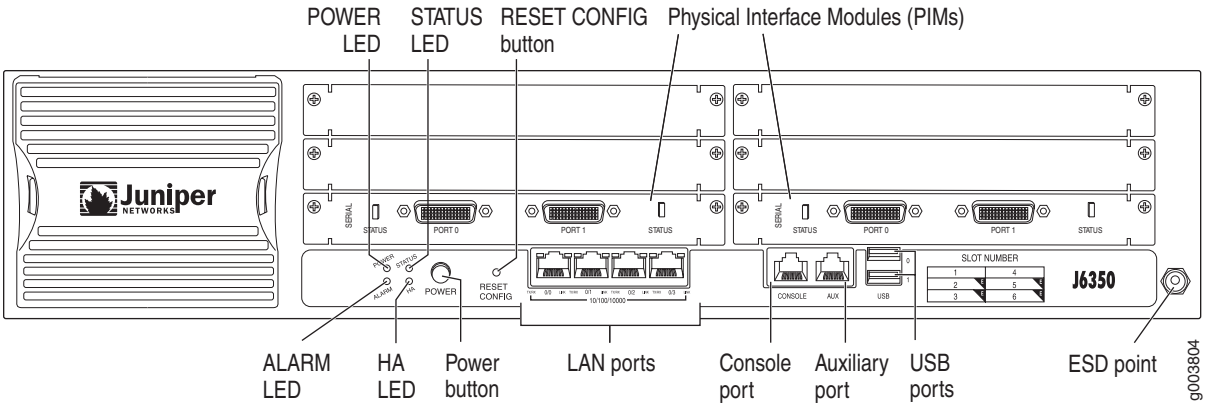
- Compact flash disk
- USB storage device

Normally, the Services Router boots from the compact flash disk. If the compact flash disk fails, the router attempts to boot from the USB storage device.

Front Panel

The front panel of the Services Router (see Figure 7) allows you to install or remove PIMs, view router status LEDs, access the console port, and perform simple control functions.

Figure 7: Front of J4350 and J6350 Chassis



The components of the front panel, from left to right, are described in the following sections:

- Physical Interface Modules (PIMs) on page 16
- Power Button and POWER LED on page 17
- STATUS LED on page 18
- ALARM LED on page 18
- HA LED on page 19
- RESET CONFIG Button on page 19
- Built-In Gigabit Ethernet Ports on page 19
- Console Port on page 20
- AUX Port on page 20
- USB Port on page 20

Physical Interface Modules (PIMs)

Physical Interface Modules (PIMs) provide the physical connection to various network media types. For information about individual PIMs, see “Field-Replaceable PIMs” on page 29.

For pinouts of PIM cable connectors, see “Network Cable Specifications and Connector Pinouts” on page 185. For PIM replacement instructions, see “Replacing a PIM” on page 144.

Each Services Router has six front panel slots for field-replaceable PIMs. These slots are numbered from top to bottom and from left to right as shown in the slot number diagram on the front panel, shown in Figure 8.

Figure 8: Slot Number Diagram on Front Panel

Gigabit Ethernet and 4-port Fast Ethernet ePIMs can be installed in high-speed slots only. High-speed slots are indicated by a black triangle containing an **E** in the front panel slot number diagram. On J4350 Services Routers, the high-speed slots are slot 3 and slot 6. On J6350 Services Routers, the high-speed slots are slots 2, 3, 5, and 6.

Slot 0 is the fixed interface module that contains the built-in Ethernet ports.

Power Button and POWER LED

The power button is located on the left side of the front panel (see Figure 7). You can use the power button to power the Services Router on and off. When you power on the router, the Routing Engine boots as the power supply completes its startup sequence.

The POWER LED is located to the upper left of the LED dashboard. Table 7 describes the POWER LED.

Table 7: POWER LED

Color	State	Description
Green	On steadily	Power is functioning correctly.
	Blinking	Power button has been pressed and quickly released, and the router is gracefully shutting down.
Unlit	Off	Router is not receiving power.

After the router is powered on, status indicators—such as LEDs on the front panel and show chassis command output—can take up to 60 seconds to indicate that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

If you need to power off the router after the Routing Engine finishes booting, use the J-Web interface or the CLI to halt the Services Router first. For instructions, see the *J-series Services Router Administration Guide*.

STATUS LED

When the system is powered on, the STATUS LED changes from off to blinking green. Startup takes approximately 90 seconds to complete. If you want to turn the system off and on again, we recommend waiting a few seconds between shutting it down and powering it back up. Table 8 describes the STATUS LED.

Table 8: Status LED

Color	State	Description
Green	Blinking	Router is starting up or performing diagnostics.
	On steadily	Router is operating normally.
Red	Blinking	Error has been detected.

ALARM LED

The ALARM LED lights yellow to indicate a minor condition that requires monitoring or maintenance and lights red to indicate a major condition that can result in a system shutdown. When the condition is corrected, the light turns off. Table 9 describes the ALARM LED.

Table 9: ALARM LED

Color	State	Description
Red	On steadily	Major alarm indicates a critical situation on the router that has resulted from one of the following conditions. A red alarm condition requires immediate action: ■ One or more hardware components have failed. ■ One or more hardware components have exceeded temperature thresholds. ■ An alarm condition configured on an interface has triggered a critical warning.
Yellow	On steadily	Minor alarm condition requires monitoring or maintenance: ■ Indicates a noncritical condition on the router that, if left unchecked, might cause an interruption in service or degradation in performance. ■ A missing rescue configuration or software license generates a yellow system alarm.
Unlit	Off	No alarms.

For information about alarm conditions and corrective actions, see “Chassis Alarm Conditions” on page 171. For additional information, see the *J-series Services Router Administration Guide*.

HA LED

The HA (high availability) LED is for future use. The LED lights when the router starts, but otherwise remains unlit.

RESET CONFIG Button

Use the RESET CONFIG button to return the router to either the rescue configuration or the factory default configuration. The button is recessed to prevent it from being pressed accidentally.

For example, if someone inadvertently commits a configuration that denies management access to a Services Router, you can delete the invalid configuration and replace it with a rescue configuration by pressing the RESET CONFIG button. You must have previously set the rescue configuration through the J-Web interface or the CLI. The rescue configuration is a previously committed, valid configuration.

CAUTION: Pressing and holding the RESET CONFIG button for 15 seconds or more—until the configuration LED blinks red—deletes *all* configurations on the router, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

You can change the default behavior of the RESET CONFIG button. For more information, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Built-In Gigabit Ethernet Ports

Four built-in Gigabit Ethernet ports provide LAN connections over copper interfaces to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic. When configuring one of these ports, you use the interface name that corresponds to the port's location. From left to right on the front panel, the interface names for the ports are ge-0/0/0, ge-0/0/1, ge-0/0/2, and ge-0/0/3.

For Gigabit Ethernet port pinout information, see "RJ-45 Connector Pinout for Gigabit Ethernet Ports" on page 195.

Each port has two LEDs, a TX/RX LED on the left side and a LINK LED on the right side. Table 10 describes the built-in Ethernet port LEDs.

Table 10: Gigabit Ethernet Port LEDs

Function	Color	State	Description
LINK	Green	On steadily	Port is online.
	Unlit	Off	Port is offline.

Table 10: Gigabit Ethernet Port LEDs (continued)

Function	Color	State	Description
TX/RX	Green	Blinking	Port is transmitting or receiving data.
	Unlit	Off	Port might be online, but it is not receiving data.

Console Port

You can use the console port to connect to the Routing Engine through an RJ-45 serial cable. From the console port, you can use the CLI to configure the router. The console port is configured as data terminal equipment (DTE) and supports the RS-232 (EIA-232) standard.

For information about securing the console port, see the *J-series Services Router Administration Guide*

For console port pinout information, see "Console Port Pinouts" on page 195. For information about securing the console port, see the *J-series Services Router Administration Guide*.

AUX Port

The port labeled AUX on the front panel of the J4350 or J6350 Services Router is for future use and is not activated.

USB Port

The USB ports on the front panel of the router (see Figure 7) accept a USB storage device or USB storage device adapter with a compact flash disk installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When a USB storage device is installed and configured, it automatically acts as a secondary boot device, if the primary compact flash disk fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a failure. For information about configuring a USB storage device, see the *J-series Services Router Administration Guide*.

NOTE: For a list of supported USB storage devices, see the *J-series Services Router Release Notes* at http://www.juniper.net.

J4350 Power System

The J4350 Services Router uses either AC or DC power. The autosensing power supply (see Figure 2 or Figure 4) distributes the different output voltages to the router components according to their voltage requirements.

The power supply is fixed in the chassis, and is not field-replaceable. The AC power supply has a single AC appliance inlet that requires a dedicated AC power feed. The DC power supply has a terminal block that provides a single DC input (–48 VDC and return) and requires a dedicated 15 A (–48 VDC) circuit breaker.

The J4350 AC-powered chassis has a power switch and does not include a power LED.

The J4350 DC-powered chassis includes a power supply LED located to the upper right of the power supply connector. Table 11 describes the power supply LED.

Table 11: Power Supply LED

State	Description
Off	No power is flowing to the power supply.
Green	Power supply is connected and power is flowing.
Yellow	Power supply is connected, but the router is not powered on.

For information about site power preparations, see “Power Guidelines, Requirements, and Specifications” on page 74. For information about connecting the router to power and ground, see “Connecting Power” on page 86.

J6350 Power System

The J6350 Services Router uses either AC or DC power. You can install one or two autosensing, load-sharing power supplies at the bottom rear of the chassis, as shown in Figure 3 or Figure 5. The power supplies distribute the different output voltages to the router components, depending on their voltage requirements. When two power supplies are installed and operational, they automatically share the electrical load.

For full redundancy, two power supplies are required. If a power supply stops functioning for any reason, the second power supply instantly begins providing all the power the router needs for normal functioning. It can provide full power indefinitely. Power supplies on the J6350 Services Router can be hot-swapped.

Each power supply has an LED located to the upper right of the power supply connector. Table 11 describes the power supply LED.

For information about site power preparations, see “Power Guidelines, Requirements, and Specifications” on page 74. For information about connecting the router to power and ground, see “Connecting Power” on page 86.

Power supplies on J6350 Services Routers are hot-removable and hot-insertable. You can remove and replace a redundant power supply without powering down the

router or disrupting the routing functions. To avoid electrical injury, carefully follow the instructions in “Replacing Power System Components” on page 158.

NOTE: You cannot mix DC and AC power supplies in the same chassis.

WARNING: DC-powered Services Routers are intended for installation only in a restricted access location.

Cooling System

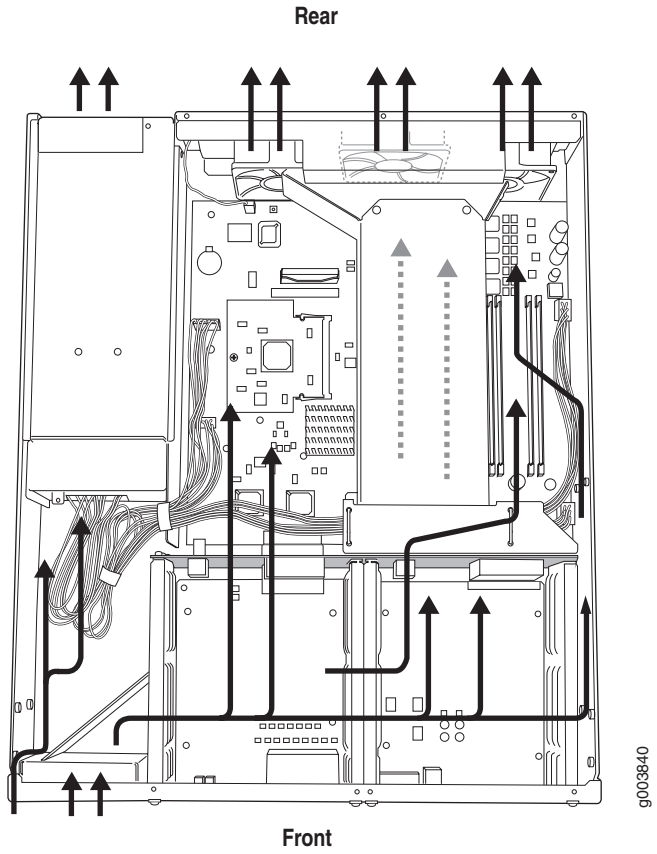
The cooling system includes three fans at the rear of the chassis. The airflow produced by these fans keeps router components within the acceptable temperature range (see Figure 9). The speed of the fans is adjusted automatically according to current temperature.

An air filter protects the air intake opening at the front of the chassis and must be replaced periodically. For instructions, see “Replacing an Air Filter” on page 170.

The Routing Engine monitors the temperature of the router components. If the ambient maximum temperature specification is exceeded and the router cannot be adequately cooled, the Routing Engine shuts down the hardware components.

An additional fan is part of each power supply. This fan is not regulated by the operating system.

Figure 9: Airflow Through the J4350 and J6350 Chassis



Software Overview

Each J-series Services Router runs the JUNOS Internet software on its general-purpose processors. Designed for the large production networks typically supported by Internet service providers (ISPs), the JUNOS software includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the router chassis.

The JUNOS Internet software runs on the Routing Engine. The Routing Engine kernel coordinates communication among the JUNOS software processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the JUNOS software, you configure the routing protocols that run on the Services Router and set the properties of its network interfaces. After activating a software configuration, use either user interface to monitor the protocol traffic passing through the router, manage operations, and diagnose protocol and network connectivity problems.

This section contains the following topics:

- Routing Engine and Packet Forwarding Engine on page 24
- Kernel and Microkernel on page 24
- JUNOS Software Processes on page 24
- User Interfaces on page 25

Routing Engine and Packet Forwarding Engine

A Services Router has two primary software processing components:

- Routing Engine—Creates and maintains the routing tables that determine how packets are routed through the network.
- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

For information about Routing Engine hardware, see "Routing Engine" on page 14.

Kernel and Microkernel

The Routing Engine kernel provides the underlying infrastructure for all JUNOS software processes by doing the following:

- Linking the routing tables maintained by the routing protocol process with the forwarding table maintained by the Routing Engine
- Coordinating communication with the Packet Forwarding Engine, primarily by synchronizing the Packet Forwarding Engine's forwarding table with the master forwarding table maintained by the Routing Engine

The microkernel contains device drivers and processes that the Packet Forwarding Engine uses to govern the flow of packets through the Services Router.

JUNOS Software Processes

The JUNOS software running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual Services Router functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the JUNOS software, for added flexibility.

Table 12 describes the primary JUNOS software processes.

Table 12: JUNOS Software Processes

Process	Name	Description
Management process	mgd	Manages the Services Router system as follows: ■ Provides communication between the other processes and an interface to the configuration database ■ Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured ■ Interacts with the other processes when commands are issued through one of the user interfaces on the router
Chassis process	chassisd	Controls a Services Router chassis and its components as follows: ■ Detects hardware on the system that is used to configure network interfaces ■ Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered ■ Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully
Routing protocol process	rpd	Defines how routing protocols such as RIP, OSPF, and BGP operate on the router, including selecting routes and maintaining fowarding tables.
Interface process (also called device control process)	dcd	Supplies the programs that configure and monitor network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.
Forwarding process	fwdd	Responsible for most of the packet transmission through a Services Router. The overall performance of the router is largely determined by the effectiveness of the forwarding process.

User Interfaces

The user interfaces on a Services Router interact with the management process to execute commands and store and retrieve information from the configuration database. The user interfaces operate as clients that communicate with the JUNOS Internet software through an application programming interface (API).

The following primary user interfaces are shipped with the router:

- J-Web graphical user interface—Includes quick configuration capabilities for performing the minimum required steps to enable a feature, plus a built-in configuration editor with access to the entire configuration hierarchy to fully

configure the router. The J-Web interface also provides tools for monitoring, managing, and diagnosing router operation.

- Command-line interface (CLI)—Grants access to the complete JUNOS command and configuration hierarchies, to monitor the router, diagnose problems, and configure it completely.

For more information, see "Services Router User Interface Overview" on page 49.

Other user interfaces for the Services Router interact with the management process through the common API interface. These interfaces are designed to facilitate the configuration of one or, in some cases, many routers on the network. Among the supported interfaces are the JUNOScope and Service Deployment System (SDX) applications. For more information about these products, see the *JUNOScope Software User Guide* and the *SDX Software Basics Guide*.

Chapter 3

Physical Interface Modules Overview

A Physical Interface Module (PIM) is a network interface card that is installed on a J-series Services Router, to provide physical connections to a LAN or a WAN. The PIM receives incoming packets from the network and transmits outgoing packets to the network. Each PIM is equipped with a dedicated network processor that forwards incoming data packets to the Routing Engine, and receives outgoing data packets from the Routing Engine. During this process, the PIM performs framing and line-speed signaling for its medium type.

WARNING: PIMs are not hot-swappable. You must power off the Services Router before removing or inserting a PIM.

For a complete list of supported PIMs, see Table 14.

For information about network interfaces, see the interfaces overview and configuration information in the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

For a J-series Services Router PIM compatibility matrix and datasheets, go to http://www.juniper.net/products/jseries/.

This chapter contains the following topics.

- PIM Terms on page 27
- Field-Replaceable PIMs on page 29

PIM Terms

To understand the PIMs, become familiar with the terms defined in Table 13.

Table 13: PIM Terms

Term	Definition
ADSL 2/2+ Annex A	ITU-T Standard G.992.1 that defines how ADSL works over plain old telephone service (POTS) lines.

Table 13: PIM Terms (continued)

Term	Definition
ADSL 2/2 + Annex B	ITU-T Standard G.992.1 that defines how ADSL works over Integrated Services Digital Network (ISDN) lines.
bandwidth on demand	ISDN cost-control feature defining the bandwidth threshold that must be reached on all links before a Services Router initiates additional ISDN data connections to provide more bandwidth.
basic rate interface (BRI)	ISDN interface intended for home and small enterprise applications. BRI consists of two 64-Kbps B-channels and one 16-Kbps D-channel.
callback	Alternative feature to dial-in that enables a J-series Services Router to call back the caller from the remote end of a backup ISDN connection. Instead of accepting a call from the remote end of the connection, the router rejects the call, waits a configured period of time, and calls a number configured on the router's dialer interface. See also *dial-in*.
caller ID	Telephone number of the caller on the remote end of a backup ISDN connection, used to dial in and also to identify the caller. Multiple caller IDs can be configured on an ISDN dialer interface. During dial-in, the router matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.
channel service unit (CSU)	Unit that connects a digital telephone line to a multiplexer or other signal service.
data service unit (DSU)	Unit that connects a data terminal equipment (DTE) device—in this case, a Services Router—to a digital telephone line.
data terminal equipment–to–data communication equipment (DTE–DCE) interface	Interface that a Services Router (the DTE) uses to exchange information with a serial device such as a modem (the DCE). A DTE cable uses a male 9-pin or 25-pin connector, and a DCE cable uses a female 9-pin or 25-pin connector.
demand circuit	Interface configured for dial-on-demand routing backup. In OSPF, the demand circuit reduces the amount of OSPF traffic by removing all OSPF protocols when the routing domain is in a steady state.
dial backup	Feature that reestablishes network connectivity through one or more backup ISDN dialer interfaces after a primary interface fails. When the primary interface is reestablished, the ISDN interface is disconnected.
dial-in	Feature that enables J-series Services Routers to receive calls from the remote end of a backup ISDN connection. The remote end of the ISDN call might be a service provider, a corporate central location, or a customer premises equipment (CPE) branch office. All incoming calls can be verified against caller IDs configured on the router's dialer interface. See also *callback*.
dialer filter	Stateless firewall filter that enables dial-on-demand routing backup when applied to a physical ISDN interface and its dialer interface configured as a passive static route. The passive static route has a lower priority than dynamic routes. If all dynamic routes to an address are lost from the routing table and the router receives a packet for that address, the dialer interface initiates an ISDN backup connection and sends the packet over it. See also *dial-on-demand routing backup; floating static route*.

Table 13: PIM Terms (continued)

Term	Definition
dial-on-demand-routing (DDR) backup	Feature that provides a J-series Services Router with full-time connectivity across an ISDN line. When routes on a primary serial T1, E1, T3, E3, Fast Ethernet, or PPPoE interface are lost, an ISDN dialer interface establishes a backup connection. To save connection time costs, the Services Router drops the ISDN connection after a configured period of inactivity. Services Router with ISDN interfaces support two types of dial-on-demand routing backup: on-demand routing with a dialer filter and dialer watch. See also *dialer filter; dialer watch*.
dialer watch	Dial-on-demand routing (DDR) backup feature that provides reliable connectivity without relying on a dialer filter to activate the ISDN interface. The ISDN dialer interface monitors the existence of each route on a watch list. If all routes on the watch list are lost from the routing table, dialer watch initiates the ISDN interface for failover connectivity. See also *dial-on-demand routing backup*.
"dying gasp" notification	Ability of a Services Router with a digital subscriber line (DSL) connection that has lost power to send a message informing the attached DSL access multiplexer (DSLAM) that it is about to go offline.
ePIM	Enhanced PIM. A particular type of high-speed PIM, such as the Gigabit Ethernet ePIM or 4-port Fast Ethernet ePIM, which can be inserted only in high-speed slots (slots 3 and 6 on a J4350 Services Router, or slots 2, 3, 5, and 6 on a J6350 Services Router).
floating static route	Route with an administrative distance greater than the administrative distance of the dynamically learned versions of the same route. The static route is used only when the dynamic routes are no longer available. When a floating static route is configured on an interface with a dialer filter, the interface can be used for backup.
ISDN S/T interface	Interface between an ISDN network and a network termination device consisting of two twisted pairs, one each for transmitting and receiving. The S/T interface usually resides in the customer premises and operates at 192 Kbps, of which ISDN traffic accounts for 144 Kbps.
ISDN U interface	Single twisted–pair interface line connecting the customer premises unit in an ISDN network to the central office. A U interface runs at 144 Kbps (128 Kbps for two B channels and 16 Kbps for the D channel).
plain old telephone service (POTS)	Standard telephone service that allows limited speed and bandwidth of 52 Kbps, which is also know as public switched telephone network (PSTN).

Field-Replaceable PIMs

PIMs are removable and insertable only when the Services Router is powered off. You can install a PIM into one of the six slots in the router chassis. If a slot is not occupied by a PIM, a PIM blank panel must be installed to shield the empty slot and to allow cooling air to circulate properly through the router.

These Services Routers support the types of PIMs summarized in Table 14 and described in the following sections:

- Field-Replaceable PIM Summary on page 30
- Gigabit Ethernet ePIMs on page 31

- Dual-Port Serial PIM on page 34
- Dual-Port T1 or E1 PIM on page 35
- Dual-Port Channelized T1 or E1 PIM on page 36
- T3 or E3 PIM on page 38
- Dual-Port Fast Ethernet PIM on page 40
- 4-Port Fast Ethernet ePIM on page 41
- 4-Port ISDN BRI PIMs on page 42
- ADSL PIM on page 44
- G.SHDSL PIM on page 46

Field-Replaceable PIM Summary

Table 14 provides software release information, slot and port numbers, and sample interface names for the field-replaceable PIMs supported on J4350 and J6350 Services Routers.

NOTE: Although J4350 and J6350 Services Routers support PIMs that were introduced before the JUNOS 8.0 release, these routers do not support software releases earlier than JUNOS 8.0.

Table 14: Field-Replaceable PIM Summary

PIM	Software Release for This PIM in J4350 or J6350	Slot and Port Numbering	Sample Interface Name (type-pim/0/port)
Gigabit Ethernet	JUNOS 8.0 and later	Can be installed on any PCI Express slot, as follows: ■ J4350: Slots 3 and 6 Port—0 ■ J6350: Slots 2, 3, 5, and 6 Port—0	ge-3/0/0
Dual-Port Serial	JUNOS 8.0 and later	Slots—1 through 6 Ports—0 and 1	se-3/0/1

Table 14: Field-Replaceable PIM Summary (continued)

PIM	Software Release for This PIM in J4350 or J6350	Slot and Port Numbering	Sample Interface Name (type-pim/0/port)
Dual-Port T1 or E1	JUNOS 8.0 and later	Slots—1 through 6 Ports—0 and 1	t1-0/0/1 or e1-0/0/1
Dual-Port Channelized T1 or Channelized E1	JUNOS 8.1 and later	Slots—1 through 6 Port—0 and 1	ct1-0/0/0 ce1-0/0/0
T3 or E3	JUNOS 8.0 and later	Slots—1 through 6 Port—0	t3-0/0/0 or e3-2/0/0
Dual-Port Fast Ethernet	JUNOS 8.0 and later	Slots—1 through 6 Ports—0 and 1	fe-1/0/0
4–port Fast Ethernet	JUNOS 8.0 and later	Can be installed on any PCI Express slot, as follows: ■ J4350: Slots 3 and 6 Ports—0 through 3 ■ J6350: Slots 2, 3, 5, and 6 Ports—0 through 3	fe-3/0/0
4-Port ISDN BRI	JUNOS 8.0 and later	Slots—1 through 6 Ports—0, 1, 2, and 3	br-1/0/2
ADSL	JUNOS 8.0 and later	Slots—1 through 6 Port—0	at-2/0/0
G.SHDSL	JUNOS 8.0 and later	Slots—1 through 6 Ports—0 and 1	at-1/0/0

Gigabit Ethernet ePIMs

In addition to the four built-in Gigabit Ethernet ports, J4350 and J6350 Services Routers also support a field-replaceable Gigabit Ethernet ePIM, which provides a physical connection to Gigabit Ethernet network media types. The field-replaceable Gigabit Ethernet ePIM is available in two versions, copper and SFP, and each version has one port.

The Gigabit Ethernet ePIM provides the following key features:

- Full-duplex and half-duplex modes (built-in and Copper Gigabit Ethernet ePIMS only)
- Autonegotiation through medium-dependent interface (MDI) and MDI crossover (MDI–X) support

Gigabit Ethernet ePIMs do not support SNMP.

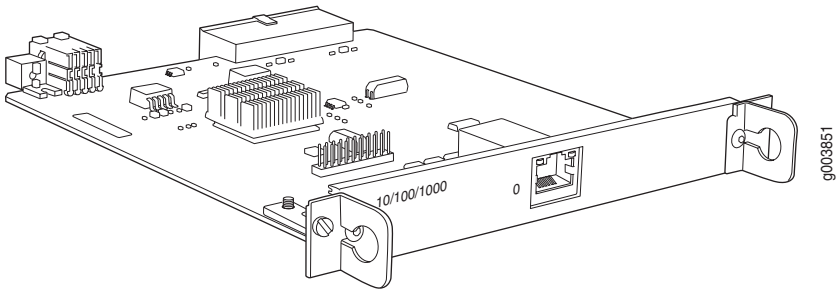
You can install Gigabit Ethernet ePIMs in any high-speed slot as follows:

- J4350—Install up to two Gigabit Ethernet ePIMs in slots 3 and 6.
- J6350—Install up to four Gigabit Ethernet ePIMs in slots 2, 3, 5, and 6.

NOTE: High speed slots are labeled with an **E** on the front-panel slot number diagram.

Figure 10 shows the Copper Gigabit Ethernet ePIM.

Figure 10: Copper Gigabit Ethernet ePIM

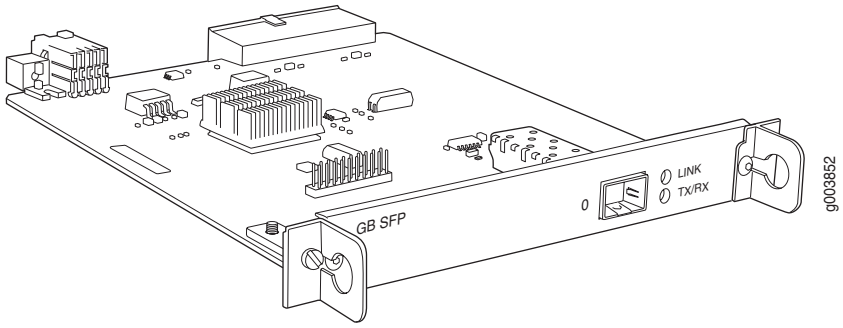


You can manually configure the Copper Gigabit Ethernet ePIM to link speeds of 10, 100, or 1000 Mbps, and you can configure the transmission mode to half or full duplex.

For pinouts of cable connectors for Gigabit Ethernet ePIMs, see “RJ-45 Connector Pinout for Gigabit Ethernet Ports” on page 195.

Figure 11 shows the SFP Gigabit Ethernet ePIM.

Figure 11: SFP Gigabit Ethernet ePIM



The SFP Gigabit Ethernet ePIM, shown in Figure 11, uses small form-factor pluggable transceivers (SFPs) that allow different interfaces to be used on the ePIM. The ePIM supports 1000Base-LX, 1000Base–SX, and 1000Base-TX SFPs only; it does not support 1000Base-LH SFPs.

The SFP Gigabit Ethernet ePIM cannot be manually configured. It is set at 1000 Mbps and full duplex.

Connect the module with a single-mode or multimode optical cable.

NOTE: Configure Gigabit Ethernet interfaces up to a maximum MTU size of 9018 bytes.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For instructions on installing and removing a PIM, see "Replacing a PIM" on page 144.

The LINK and TX/RX LEDs indicate link status and activity. Table 15 describes the meaning of the LEDs.

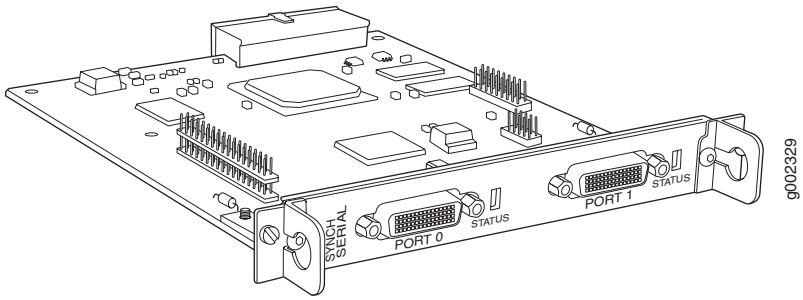
Table 15: Gigabit Ethernet Port LEDs

Function	Color	State	Description
LINK	Green	On steadily	Port is online.
	Unlit	Off	Port is offline.
TX/RX	Green	Blinking	Port is transmitting or receiving traffic.
	Unlit	Off	Port might be online, but it is not receiving traffic.

Dual-Port Serial PIM

The Dual-Port Serial PIM (Figure 12) provides a physical connection to serial network media types through two serial interface ports.

Figure 12: Dual-Port Serial PIM



The Dual-Port Serial PIM provides the following key features:

- Onboard network processor
- Autoselection of operation modes based on data terminal equipment (DTE) or data communication equipment (DCE) cables
- Local and remote loopback diagnostics
- Configurable clock rate for the transmit (Tx) clock and receive (Rx) clock

For pinouts of cable connectors for serial PIMs, see "Serial PIM Cable Specifications" on page 185.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see "Replacing a PIM" on page 144.

Status LEDs indicate port status. Table 16 describes the meaning of the LED states.

Table 16: Status LEDs for Serial Ports

Color	State	Description
Green	On steadily	Online with no alarms or failures.

Table 16: Status LEDs for Serial Ports (continued)

Color	State	Description
Red	On steadily	Active with a local alarm. The router has detected a failure.
Unlit	Off	Offline.

Dual-Port T1 or E1 PIM

The Dual-Port T1 PIM (Figure 13) and Dual-Port E1 PIM (Figure 14) provide a physical connection to T1 or E1 network media types. Each PIM has two physical T1 or E1 ports with an integrated channel service unit (CSU) or data service unit (DSU).

Figure 13: Dual-Port T1 PIM

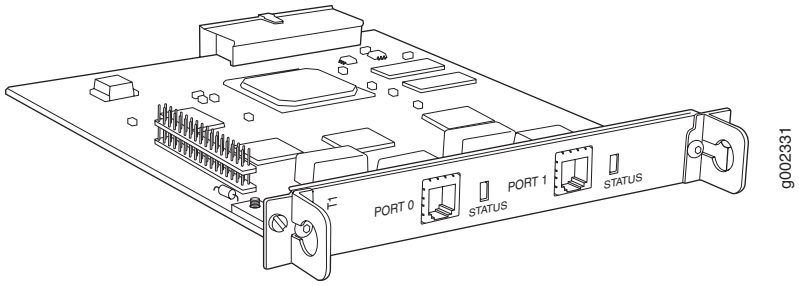
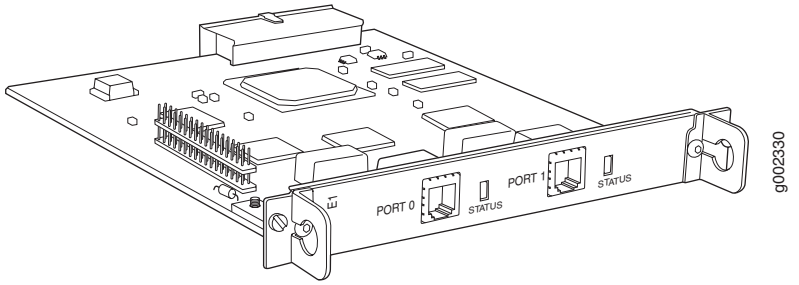


Figure 14: Dual-Port E1 PIM



The Dual-Port T1 and E1 PIMs provides the following key features:

- Onboard network processor
- Integrated CSU/DSU—Eliminates the need for a separate external device
- 56-Kbps and 64-Kbps modes
- ANSI T1.102, T1.107, and T1.403 standards compliance

- G.703, G.704, and G.706 E1 standards compliance
- Independent internal and external clocking system
- Loopback, bit error rate test (BERT), T1 facilities data link (FDL), and long buildout diagnostics

For pinouts of cable connectors for T1 and E1 PIMs, see "E1 and T1 RJ-48 Cable Pinouts" on page 196.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see "Replacing a PIM" on page 144.

Status LEDs indicate port status. Table 17 describes the meaning of the LED states.

Table 17: Status LEDs for T1 and E1 Ports

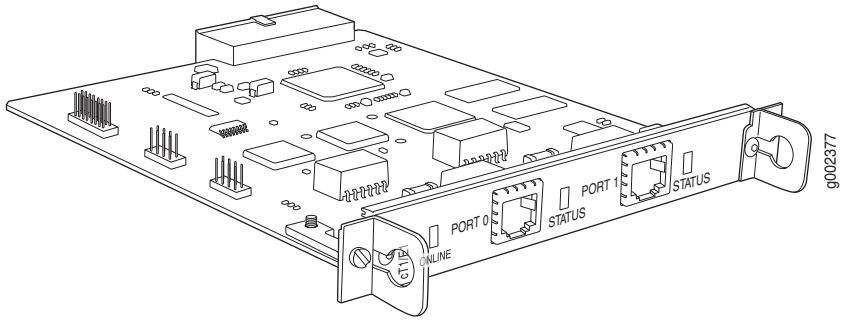
Color	State	Description
Green	On steadily	Online with no alarms or failures.
Red	On steadily	Active with a local alarm. The router has detected a failure.
Unlit	Off	Offline.

Dual-Port Channelized T1 or E1 PIM

The Dual-Port Channelized T1 or E1 PIM (Figure 15) is a multiflex interface card that allows you to configure a single interface as a channelized T1 interface or a channelized E1 interface. The channelized T1 or E1 interface supports up to 24 DS0 channels on a T1 interface and up to 32 DS0 channels on an E1 interface, in addition to supporting the features of regular (unchannelized) T1 and E1 PIMs. Each interface can be configured as a single clear channel, fractionalized, or channelized interface.

NOTE: You cannot configure a channelized T1 or E1 interface through a J-Web Quick Configuration page.

Figure 15: Channelized T1/E1 PIM



The Dual-Port Channelized T1 or E1 PIM provides the following key features:

- Onboard network processor
- Two-port channelization
- Interfaces that are software configurable as T1 or E1
- Clear-channel, fractional, and channelized operation
- Lower latency due to the addition of a Freescale processor
- Maximum MTU value of 4500 bytes (for channelized T1 or E1 interface)

NOTE: For a clear-channel T1 or E1 interface, the maximum MTU is 9150 bytes.

- 56-Kbps and 64-Kbps modes
- ANSI T1.102, T1.107, and T1.403 standards compliance
- G.703, G.704, and G.706 E1 standards compliance
- Independent internal and external clocking system
- Loopback, bit error rate test (BERT), T1 facilities data link (FDL), and long buildout diagnostics

For pinouts of cable connectors for channelized T1 and E1 PIMs, see “E1 and T1 RJ-48 Cable Pinouts” on page 196.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see “Replacing a PIM” on page 144.

Channelized T1 and E1 LEDs indicate PIM and port status. Table 18 describes the meaning of the LED states.

Table 18: LEDs for Channelized T1 and E1 PIMs

Label	Color	State	Description
ONLINE	Green	On steadily	PIM is online and operational.
	Unlit	Off	PIM is not online.
STATUS	Green	On steadily	Port is online with no alarms or failures, and the physical layer is active.
	Red	Online	Port is active with a local alarm. The router has detected a failure and the physical layer is inactive.
	Yellow	Online	Port is online with alarms for remote failures.
	Unlit	Offline	Port is disabled.

T3 or E3 PIM

The T3 (also known as DS3) PIM (Figure 16) and E3 PIM (Figure 17) provide a physical connection to T3 or E3 network media types. The T3 and E3 PIMs include one physical T3 or E3 port with an integrated data service unit (DSU).

Figure 16: T3 PIM

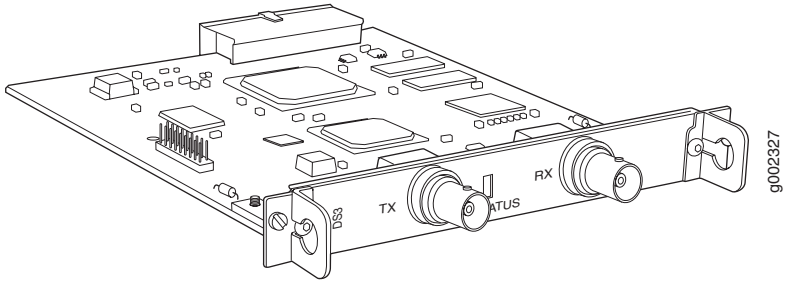
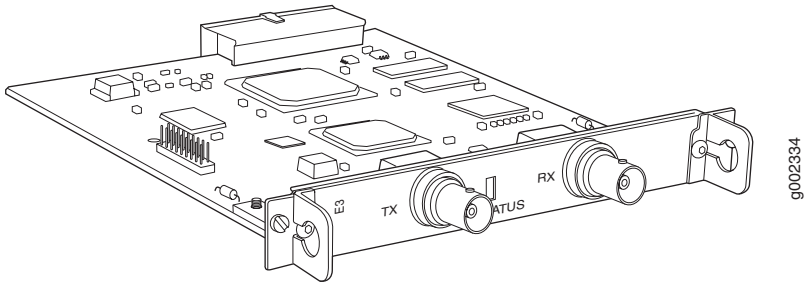


Figure 17: E3 PIM



The T3 and E3 PIMs provide the following key features:

- Onboard network processor
- Integrated DSU—Eliminates the need for a separate external device
- Subrate and scrambling options with support for major DSU vendors
- Independent internal and external clocking system
- Loopback (payload–supported only on T3 PIM, local, and remote), bit error rate test (BERT), and T3 far-end alarm and control (FEAC) diagnostics

For pinouts of cable connectors for T3 and E3 PIMs, see "E3 and T3 BNC Connector Pinout" on page 198.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see "Replacing a PIM" on page 144.

Status LEDs indicate port status. Table 19 describes the meaning of the LED states.

Table 19: Status LEDs for T3 and E3 Ports

Color	State	Description
Green	On steadily	Online with no alarms or failures.
Red	On steadily	Active with a local alarm. The router has detected a failure.

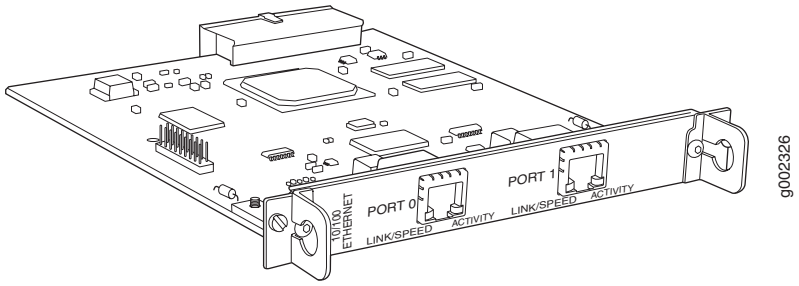
Table 19: Status LEDs for T3 and E3 Ports (continued)

Color	State	Description
Yellow	On steadily	■ Loopback mode. ■ T3 (DS3)—Remote endpoint is in red alarm failure. ■ E3—Remote defect indication (RDI).
Unlit	Off	Offline.

Dual-Port Fast Ethernet PIM

The Dual-Port 10/100-Mbps Fast Ethernet PIM (Figure 18) has two physical Fast Ethernet ports.

Figure 18: Fast Ethernet PIM



The Dual-Port Fast Ethernet PIM provides the following key features:

- Onboard network processor
- Full-duplex and half-duplex modes
- Media access control (MAC) address filtering
- Autonegotiation through medium-dependent interface (MDI) and MDI crossover (MDI–X) support

For pinouts of cable connectors for Fast Ethernet PIMs, see “RJ-45 Connector Pinout for Fast Ethernet Ports” on page 194.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see “Replacing a PIM” on page 144.

Fast Ethernet LEDs indicate link status, port speed, and activity. Table 20 describes the meaning of the LEDs.

Table 20: LEDs for Dual-Port Fast Ethernet PIM

Label	Color	State	Description
LINK/SPEED	Green (100 Mbps) Yellow (10 Mbps)	On steadily	Online and link is active.
	Red	Disconnected	Link is unavailable.
ACTIVITY	Green	Blinking	Online with network traffic.
	Green	On steadily	Online without traffic.

4-Port Fast Ethernet ePIM

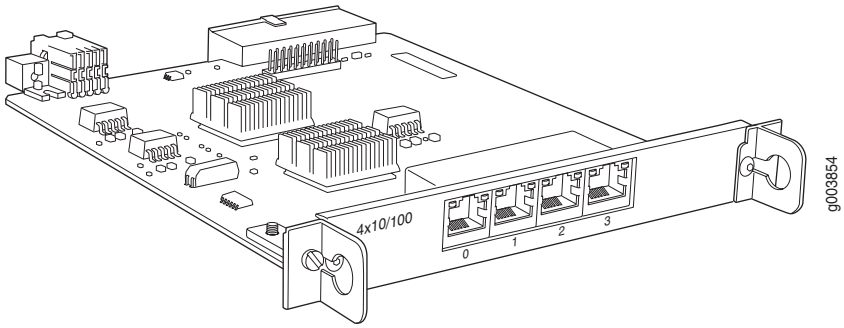
You can install 4-Port Fast Ethernet ePIMs in any of the high-speed slots, as follows:

- J4350—Install up to two 4-Port Fast Ethernet ePIMs in slots 3 and 6.
- J6350—Install up to four 4-Port Fast Ethernet ePIMs in slots 2, 3, 5, and 6.

NOTE: For 4-port Fast Ethernet ePIMs, if you apply a CoS scheduler map on outgoing (egress) traffic, the router does not divide the bandwidth appropriately among the CoS queues. As a workaround, configure enforced CoS shaping on the ports.

The 4-Port 10/100-Mbps Fast Ethernet ePIM, shown in Figure 19, has four physical Fast Ethernet ports.

Figure 19: 4-Port Fast Ethernet ePIM



The 4-Port Fast Ethernet ePIM provides the following key features:

- Full-duplex and half-duplex modes.
- Autonegotiation through medium-dependent interface (MDI) and MDI crossover (MDI–X) support.

For pinouts of cable connectors for Fast Ethernet ePIMs, see "RJ-45 Connector Pinout for Fast Ethernet Ports" on page 194.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

NOTE: 4-port Fast Ethernet ePIMs support a maximum frame size of 1514 bytes. Jumbo frames are not supported.

For information about installing and removing a PIM, see "Replacing a PIM" on page 144.

Fast Ethernet LEDs indicate link status and activity. Table 21 describes the meaning of the LEDs.

Table 21: LEDs for 4-Port Fast Ethernet ePIM

Label	Color	State	Description
Link status (upper left)	Green	On steadily	Port is online.
	Unlit	Off	Port is offline.
Link activity (upper right)	Green	Blinking	Port is transmitting or receiving data.
	Unlit	Off	Port might be online, but it is not transmitting or receiving data.

4-Port ISDN BRI PIMs

The 4-port ISDN BRI PIMs have four physical ports that support the ISDN BRI S/T (Figure 20) or ISDN BRI U (Figure 21) interface type.

Figure 20: ISDN BRI S/T PIM

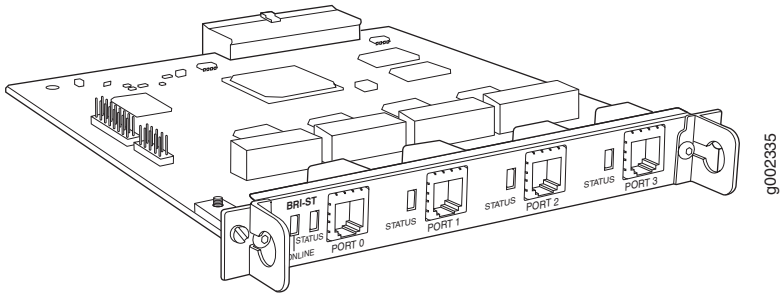
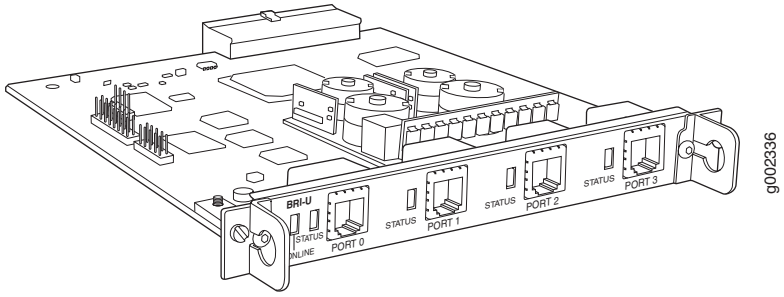


Figure 21: ISDN BRI U PIM



ISDN BRI PIMs provide the following key features:

- Onboard network processor
- Bandwidth on demand
- Dial backup
- Dial-on-demand routing backup (floating static and dialer watch)

For pinouts of cable connectors for ISDN PIMs, see “ISDN RJ-45 Connector Pinout” on page 199.

For installing and removing a PIM, see “Replacing a PIM” on page 144.

ISDN LEDs indicate PIM and port status. Table 22 describes the meaning of the LED states.

Table 22: LEDs for ISDN BRI S/T and U PIMs

Label	Color	State	Description
ONLINE	Green	Blinking	Call setup is successful on either the B1 or B2 channel.
	Green	On steadily	ISDN Layer 2 is active.
	Amber	On steadily	■ ISDN Layer 1 is active. ■ ISDN Layer 2 is unavailable.
	Red	Disconnected	■ BRI interface port is not connected. ■ ISDN Layer 1 is unavailable.
	Unlit	Off	BRI interface is offline.
STATUS	Green	On steadily	PIM is online and operational.
	Red	Disconnected	PIM is not operational and needs replacement.
	Unlit	Off	PIM is offline.

ADSL PIM

The ADSL PIM provides a single physical interface to asymmetric digital subscriber line (ADSL) network media types. The ADSL PIM, one supporting Annex A (Figure 22) over plain old telephone service (POTS) and the other Annex B (Figure 23) over ISDN, includes one physical ADSL port for an ATM-over-ADSL connection.

Figure 22: ADSL 2/2+ Annex A PIM

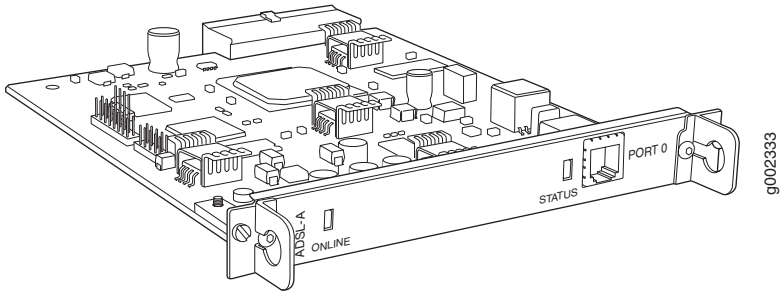
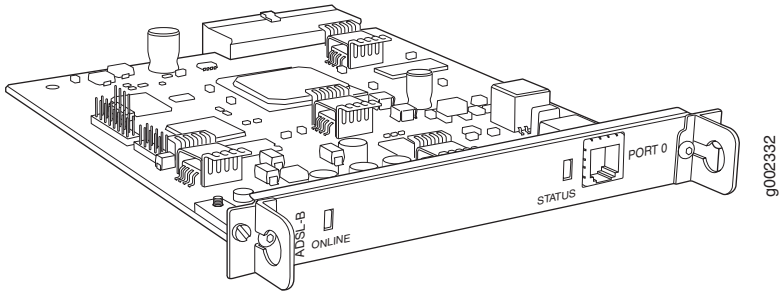


Figure 23: ADSL 2/2+ Annex B PIM



The ADSL PIM provides the following key features:

- Onboard network processor
- ADSL, ADSL2, and ADSL2 + protocols on the same PIM
- “Dying gasp” notification
- Asynchronous Transfer Mode (ATM) Adaptation Layer 5 (AAL5) encapsulation

For pinouts of cable connectors for ADSL PIMs, see “ADSL and G.SHDSL RJ-11 Connector Pinout” on page 199.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see “Replacing a PIM” on page 144.

The ADSL PIMs have two LEDs to indicate the status of the PIM and its port. Table 23 describes the meaning of the LED states.

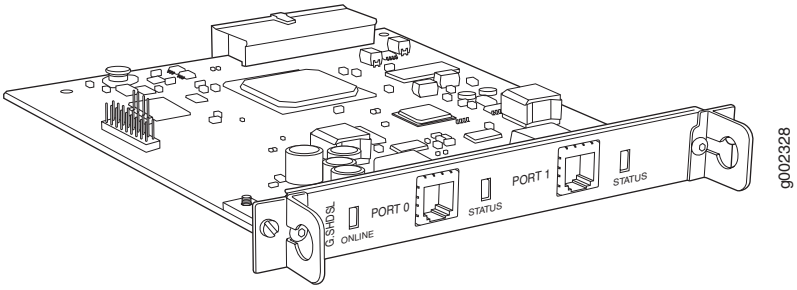
Table 23: LEDs for ADSL PIMs

Label	Color	State	Description
ONLINE	Green	On steadily	PIM passed the self-test and is online and operational.
	Unlit	Off	PIM is offline.
STATUS	Green	On steadily	Online with no alarms or failures.
	Red	On steadily	Active with local or remote alarms. The router has detected a failure.

G.SHDSL PIM

The G.SHDSL PIM (Figure 24) provides symmetric high-speed digital subscriber line (SHDSL) physical interfaces to ATM network media types. The G.SHDSL PIM has two ports for ATM-over-SHDSL connections.

Figure 24: G.SHDSL PIM



The G.SHDSL PIM supports the following key features:

- Onboard network processor
- 2-port two-wire mode and 1-port four-wire mode
- Programmable line rates in both modes:
  - 2-port two-wire mode supports autodetection of line rate and fixed line rates from 192 Kbps to 2.304 Mbps in 64-Kbps increments.
  - 1-port four-wire mode supports fixed line rates from 384 Kbps to 4.608 Mbps in 128-Kbps increments.
- 32 virtual channels per PIM
- ATM-over-G.SHDSL framing
- “Dying gasp” notification
- Local and remote loopback diagnostics
- ITU-T G.991.2, ITU-T G.994.1, and ITU-T G.997.1 standards compliance

For pinouts of cable connectors for G.SHDSL PIMs, see “ADSL and G.SHDSL RJ-11 Connector Pinout” on page 199.

For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

For installing and removing a PIM, see “Replacing a PIM” on page 144.

The G.SHDSL PIM has two LEDs to indicate the status of the PIM and its ports. Table 24 describes the meaning of the LED states.

Table 24: LEDs for G.SHDSL PIMs

Label	Color	State	Description
ONLINE	Green	On steadily	Online with no alarms or failures.
	Red	Disconnected	Initialization of the PIM has failed.
	Unlit	Off	PIM is booting.
STATUS	Green	On steadily	Online with no alarms or failures.
	Red	On steadily	Active with a local alarm. The router has detected a failure.

Chapter 4

Services Router User Interface Overview

You can use two user interfaces to monitor, configure, troubleshoot, and manage a Services Router—the J-Web interface and the JUNOS command-line interface (CLI). This chapter contains the following topics:

- User Interface Overview on page 49
- Before You Begin on page 52
- Using the J-Web Interface on page 52
- Using the Command-Line Interface on page 58

User Interface Overview

This section contains the following topics:

- J-Web Overview on page 49
- CLI Overview on page 50
- Comparison of Configuration Interfaces on page 50

J-Web Overview

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

The J-Web interface provides two methods of Services Router configuration:

- Quick Configuration
- Configuration editor

For more information, see “Comparison of Configuration Interfaces” on page 50.

In addition to configuration, you can use the J-Web interface to perform many monitoring, troubleshooting, and management tasks on the Services

Router. For example, to display a summary of routing table entries, click **Monitor** in the task bar, then click **Routing > Route Information** in the side pane. The routes are displayed in the main pane.

For more information about the J-Web interface, see "Using the J-Web Interface" on page 52.

CLI Overview

The CLI is a straightforward command interface in which you type commands on a line and press Enter to execute them. The CLI provides command help, command completion, and Emacs-style keyboard sequences for moving around on the command line and scrolling through a buffer of recently executed commands.

The CLI has two modes:

- Operational mode—Complete set of commands to control the CLI environment, monitor and troubleshoot network connectivity, manage the Services Router, and enter configuration mode.
- Configuration mode—Complete set of commands to configure the Services Router. This guide refers to configuration mode as the *CLI configuration editor*. For more information, see "Comparison of Configuration Interfaces" on page 50.

For more information about the CLI, see "Using the Command-Line Interface" on page 58.

Comparison of Configuration Interfaces

Table 25 describes and compares the interfaces you can use to configure a Services Router.

Table 25: Services Router Configuration Interfaces

Interface	Description	Capabilities	Recommendations
J-Web Quick Configuration	Web browser pages for setting up the Services Router quickly and easily without configuring each statement individually. For example, use the Set Up Quick Configuration page to configure the Services Router for basic connectivity so you can manage it from the network.	Configure basic router services: ■ Setup ■ Secure access ■ Interfaces ■ User access ■ SNMP notifications ■ Routing and protocols, including data link switching (DLSw) ■ Class of service (CoS) ■ Security firewall filters and Network Address Translation (NAT) ■ Dynamic Host Configuration Protocol (DHCP) services ■ IPSec tunnels ■ Real-time performance monitoring ■ Input and output firewall filters (ACLs)	Use for basic configuration.

Table 25: Services Router Configuration Interfaces (continued)

Interface	Description	Capabilities	Recommendations
J-Web configuration editor	Web browser pages divided into panes in which you can do any of the following: ■ Expand the entire configuration hierarchy and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option. ■ Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines. ■ Upload or download a complete configuration. ■ Roll back to a previous configuration. ■ Create or delete a rescue configuration.	Configure all router services: ■ System parameters ■ User access and accounting ■ Interfaces ■ SNMP network management ■ Routing options, including multicast routing ■ Routing protocols ■ Routing policies ■ Secure access ■ Service interfaces, including stateful firewalls and virtual private networks (VPNs) ■ Traffic engineering, including Multiprotocol Label Switching (MPLS) and class-of-service (CoS) packet prioritization ■ Chassis properties	Use for complete configuration if you are not familiar with the JUNOS CLI or prefer a graphical interface.
CLI configuration editor	Interface in which you do either of the following: ■ Type commands on a line and press Enter to create a hierarchy of configuration statements. ■ Create an ASCII text file that contains the statement hierarchy. ■ Upload a complete configuration, or roll back to a previous configuration. ■ Create or delete a rescue configuration.		Use for complete configuration if you know the JUNOS CLI or prefer a command interface.

Before You Begin

Before you start the user interface, you must perform the initial Services Router configuration described in “Establishing Basic Connectivity” on page 93. After the initial configuration, you use your username and password, and the hostname or IP address of the router, to start the user interface.

Using the J-Web Interface

This section contains the following topics:

- Starting the J-Web Interface on page 53
- J-Web Layout on page 53
- J-Web Sessions on page 58

Starting the J-Web Interface

To start the J-Web interface:

1. Launch your HTTP-enabled or HTTPS-enabled Web browser.

   To use HTTPS, you must have installed a certificate on the Services Router and enabled HTTPS.

NOTE: If the Services Router is running the worldwide version of the JUNOS Internet software and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the Services Router.

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

   The J-Web login page appears.

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

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

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

   The J-Web **Quick Configuration > Set Up** (see Figure 25) or **Monitor > System** page appears.

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

J-Web Layout

Each page of the J-Web interface is divided into the following panes shown in Figure 25 and Figure 26:

- Top pane—Displays identifying information and links.

- Main pane—Location where you monitor, configure, diagnose, and manage the Services Router by entering information in text boxes, making selections, and clicking buttons.

- Side pane—Displays suboptions of the Monitor, Configuration, Diagnose, or Manage task currently displayed in the main pane. Click a suboption to access it in the main pane.

- Bottom pane—Displays copyright and trademark information.

The layout of the panes allows you to quickly navigate through the interface. Table 26 summarizes the elements of the J-Web interface.

You navigate the J-Web interface, move forward and backward, scroll pages, and expand and collapse elements as you do in a typical Web browser interface.

Figure 25: J-Web Layout

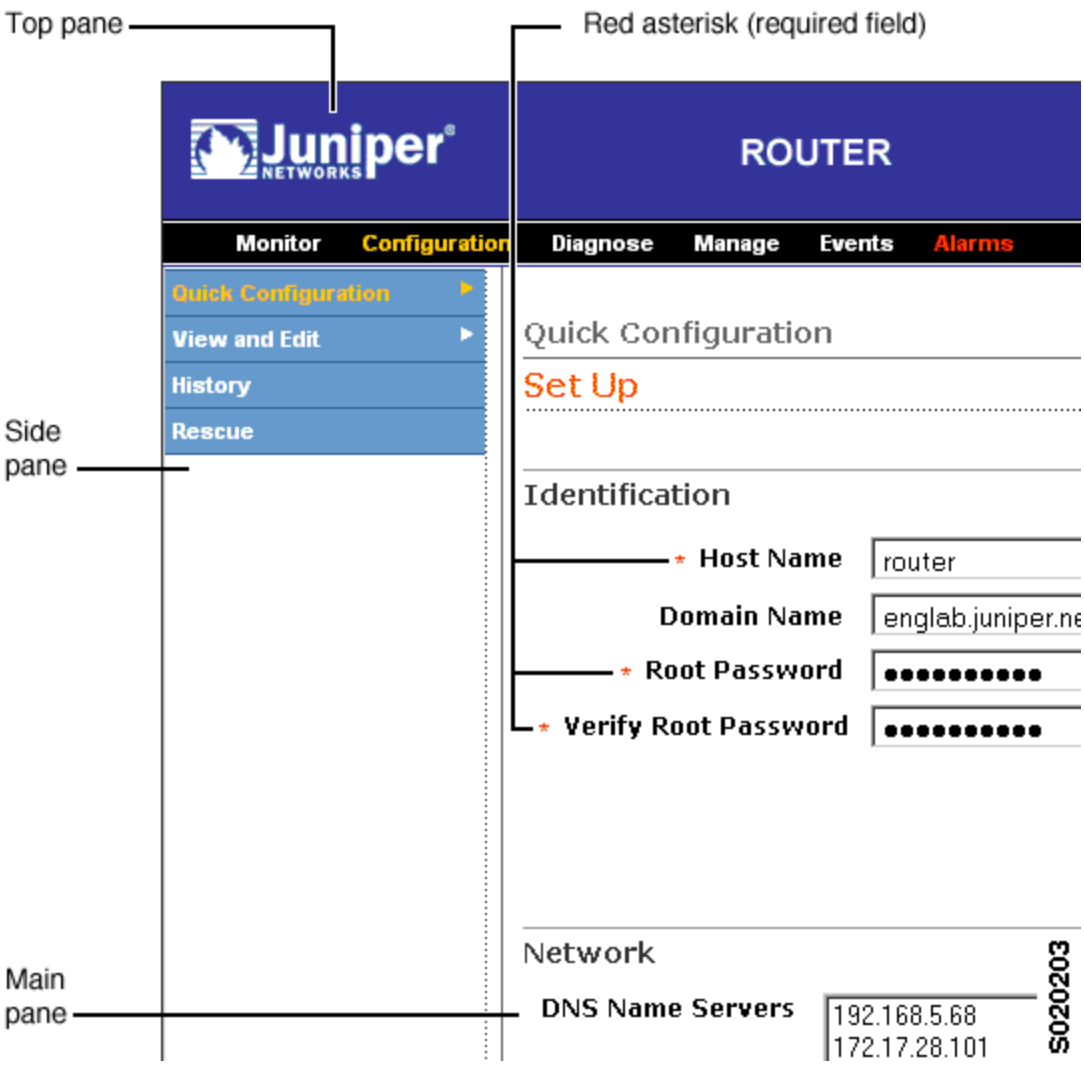


Figure 26: J-Web Layout—Configuration Editor

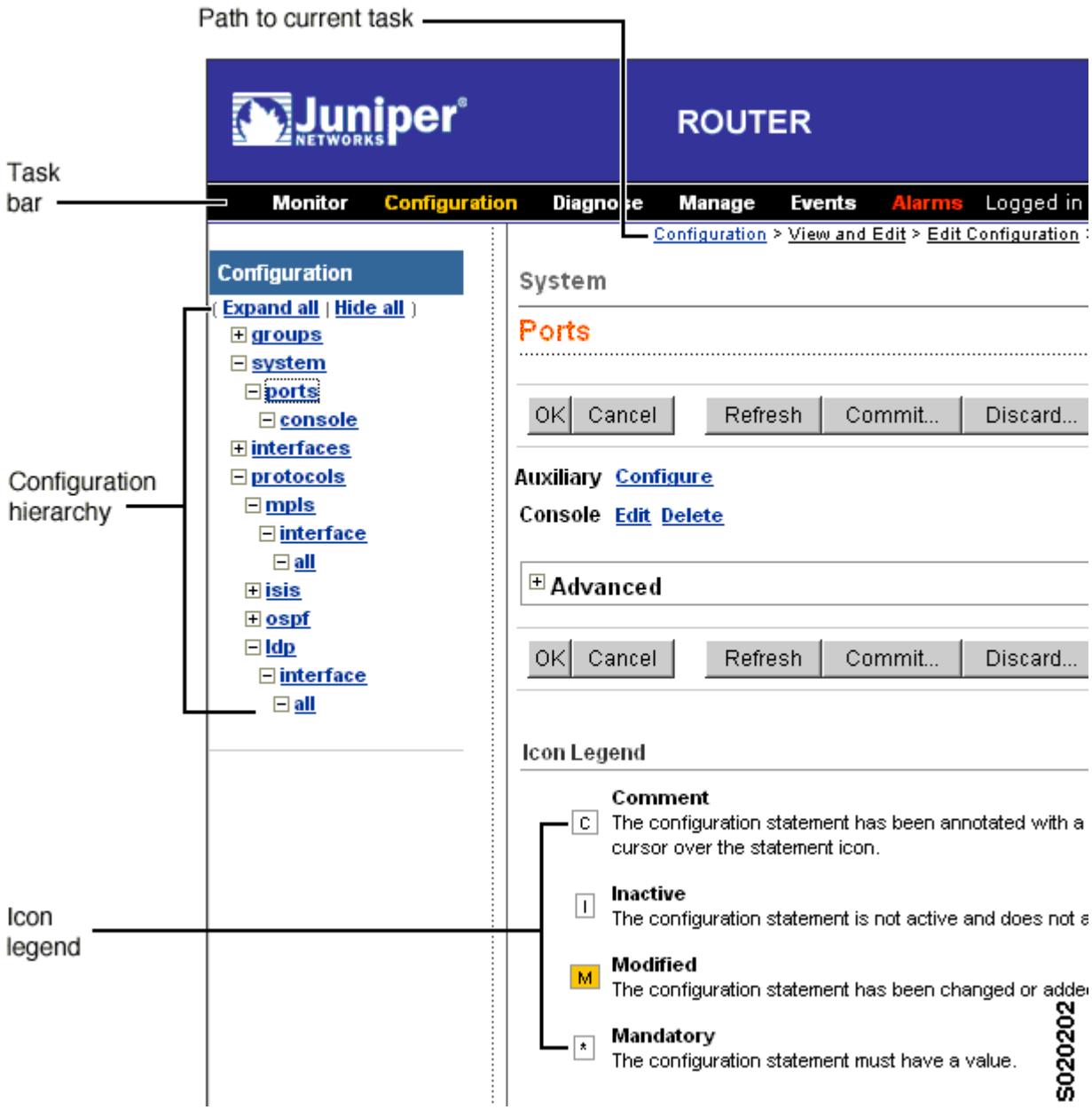


Table 26: Summary of J-Web Elements

J-Web Interface Element	Description
Top Pane	
Juniper Networks logo	Link to http://www.juniper.net in a new browser window.
hostname – model	Hostname and model of the Services Router.
Logged in as: *username*	Username you used to log in to the Services Router.
Help	Link to context-sensitive help information.
About	Displays information about the J-Web interface, such as the version number.
Logout	Ends your current login session with the Services Router and returns you to the login page.
Task bar	Menu of J-Web main options. Click to access. ■ **Monitor**—View information about configuration and hardware on the Services Router. ■ **Configuration**—Configure the Services Router with Quick Configuration or the configuration editor, and view configuration history. ■ **Diagnose**—Troubleshoot network connectivity problems. ■ **Manage**—Manage files and licenses, upgrade software, and reboot the Services Router. ■ **Events**—View events and set up filters for an event summary. ■ **Alarms**—View the alarm summary.
Main Pane	
Help (?) icon	Displays useful information—such as the definition, format, and valid range of an option—when you move the cursor over the question mark.
Red asterisk (*)	Indicates a required field.
Path to current task	Path of main options and suboptions you selected to display the current main and side panes.
Icon Legend	(Applies to the configuration editor only) Explains icons that appear in the user interface to provide information about configuration statements: ■ C—Comment. Move your cursor over the icon to view a comment about the configuration statement. ■ I—Inactive. The configuration statement does not affect the Services Router. ■ M—Modified. The configuration statement is added or modified. ■ *—Mandatory. The configuration statement must have a value.
Side Pane	
Configuration hierarchy	(Applies to the configuration editor only) Displays the hierarchy of committed statements in the Services Router configuration. ■ Click **Expand all** to display the entire hierarchy. ■ Click **Hide all** to display only the statements at the top level. ■ Click plus signs (+) to expand individual items. ■ Click minus signs (-) to hide individual items.

J-Web Sessions

You establish a J-Web session with the Services Router through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the JUNOS software. To use HTTPS, you must have installed a certificate on the Services Router and enabled HTTPS.

When you attempt to log in through the J-Web interface, the Services Router authenticates your username with the same methods used for Telnet and SSH.

The Services Router can support multiple J-Web sessions for a single user who logs in to each session. However, if a single user attempts to launch multiple J-Web *windows*—for example, by right-clicking a link to launch another instance of a Web browser—the session can have unpredictable results.

If the Services Router does not detect any activity through the J-Web interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

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

Using the Command-Line Interface

This section contains the following topics:

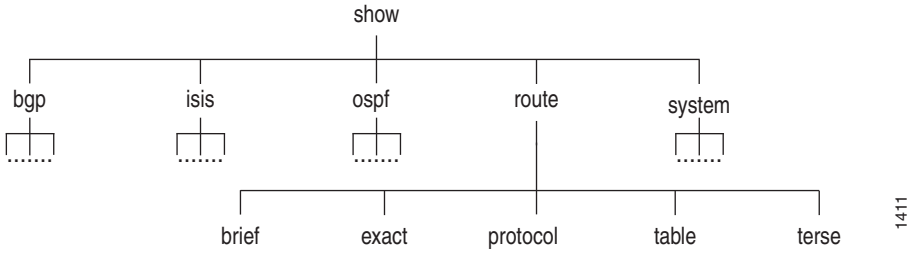
- CLI Command Hierarchy on page 58
- Starting the CLI on page 59
- CLI Operational Mode on page 60
- CLI Configuration Mode on page 61
- CLI Basics on page 62

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

CLI Command Hierarchy

The CLI commands are organized hierarchically, with commands that perform a similar function grouped together under the same level. For example, all commands that display information about the Services Router system and system software are grouped under the show command, and all commands that display information about the routing table are grouped under the show route command. Figure 27 illustrates a portion of the show command hierarchy.

Figure 27: CLI Command Hierarchy Example



To execute a command, you enter the full command name, starting at the top level of the hierarchy. For example, to display a brief view of the routes in the routing table, use the command show route brief.

The hierarchical organization results in commands that have a regular syntax and provides the following features that simplify CLI use:

- Consistent command names—Commands that provide the same type of function have the same name, regardless of the portion of the software they are operating on. For example, all show commands display software information and statistics, and all clear commands erase various types of system information.
- Lists and short descriptions of available commands—Information about available commands is provided at each level of the CLI command hierarchy. If you type a question mark (?) at any level, you see a list of the available commands along with a short description of each command.
- Command completion—Command completion for command names (keywords) and command options is also available at each level of the hierarchy. If you type a partial command name followed immediately by a question mark (with no intervening space), you see a list of commands that match the partial name you typed.

Starting the CLI

To start the CLI:

1. Establish a connection with the Services Router:
   - To access the router remotely from the network, enter the command you typically use to establish a remote connection (such as Telnet or ssh) using the router hostname.
   - To access the router through a management device attached to the console port, start the terminal application.
2. Log in using your username and password.

   After you log in, you enter a UNIX shell.

3. Start the CLI.

```
user# cli
user@host>
```

The presence of the angle bracket (>) prompt indicates the CLI has started. By default, the prompt is preceded by a string that contains your username and the hostname of the Services Router.

To exit the CLI and return to the UNIX shell, enter the quit command.

CLI Operational Mode

The CLI has two modes: *operational* and *configuration*. When you log in to the Services Router and the CLI starts, you are at the top level of operational mode.

To view a list of top-level operational mode commands, type a question mark (?) at the command-line prompt.

```
    user@host> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

At the top level of operational mode are a number of broad groups of CLI commands that are used to perform the following functions:

- Control the CLI environment.
- Monitor and troubleshoot the router.
- Connect to other systems.
- Manage files and software images.
- Control software processes.
- Stop and reboot the router.
- Enter configuration mode.

To control the CLI environment, see “Configuring the CLI Environment” on page 65. To enter configuration mode, see “CLI Configuration Mode” on page 61. For information about the other CLI operational mode functions, see the *J-series Services Router Administration Guide*.

CLI Configuration Mode

To configure the Services Router, including system parameters, routing protocols, interfaces, network management, and user access, you must enter configuration mode. In configuration mode, the CLI provides commands to configure the router, load a text (ASCII) file that contains the router configuration, activate a configuration, and save the configuration to a text file.

You enter configuration mode by entering the configure operational mode command. The CLI prompt changes from user@host> to user@host#.

To view a list of configuration mode commands, type a question mark (?) at the command-line prompt. (You do not need to press Enter after typing the question mark.)

```
    user@host# ?
Possible completions:
  Enter                Execute this command
  activate             Remove the inactive tag from a statement
  annotate             Annotate the statement with a comment
  commit               Commit current set of changes
  copy                 Copy a statement
  deactivate           Add the inactive tag to a statement
  delete               Delete a data element
  edit                 Edit a sub-element
  exit                 Exit from this level
  help                 Provide help information
  insert               Insert a new ordered data element
  load                 Load configuration from ASCII file
  quit                 Quit from this level
  rename               Rename a statement
  rollback             Roll back to previous committed configuration
  run                  Run an operational-mode command
  save                 Save configuration to ASCII file
  set                  Set a parameter
  show                 Show a parameter
  status               Show users currently editing configuration
  top                  Exit to top level of configuration
  up                   Exit one level of configuration
  wildcard             Wildcard operations
```

The JUNOS software configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which contain other statements, and *leaf statements*, which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.

Each statement consists of a fixed keyword and, optionally, an identifier that you define, such as the name of an interface or a username.

To configure the Services Router or to modify an existing configuration, you add statements to the configuration with the edit and set configuration mode commands. For more information about the CLI configuration editor and configuration mode, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide* and the JUNOS software configuration guides.

CLI Basics

This section contains the following topics:

- Editing Keystrokes on page 62
- Command Completion on page 63
- Online Help on page 63
- Configuring the CLI Environment on page 65

Editing Keystrokes

In the CLI, you use keystrokes to move around on and edit the command line, and to scroll through a list of recently executed commands. Table 27 lists some typical CLI editing tasks and the keystrokes that perform them.

Table 27: CLI Editing Keystrokes

Task Category	Action	Keyboard Sequence
Move the cursor.	Move the cursor back one character.	Ctrl-b
	Move the cursor back one word.	Esc b
	Move the cursor forward one character.	Ctrl-f
	Move the cursor forward one word.	Esc f
	Move the cursor to the end of the command line.	Ctrl-e
Delete characters.	Delete the character before the cursor.	Ctrl-h, Delete, or Backspace
	Delete the character at the cursor.	Ctrl-d
	Delete all characters from the cursor to the end of the command line.	Ctrl-k
	Delete all characters on the command line.	Ctrl-u or Ctrl-x
	Delete the word before the cursor.	Ctrl-w or Esc Backspace
	Delete the word after the cursor.	Esc d
Insert recently deleted text.	Insert the most recently deleted text at the cursor.	Ctrl-y
Redraw the screen.	Redraw the current line.	Ctrl-l

Table 27: CLI Editing Keystrokes (continued)

Task Category	Action	Keyboard Sequence
Display previous command lines.	Scroll backward through the list of recently executed commands.	Ctrl-p
	Scroll forward through the list of recently executed commands.	Ctrl-n
	Search the CLI history in reverse order for lines matching the search string.	Ctrl-r
	Search the CLI history by typing some text at the prompt, followed by the keyboard sequence. The CLI attempts to expand the text into the most recent word in the history for which the text is a prefix.	Esc /
Repeat keyboard sequences.	Specify the number of times to execute a keyboard sequence. Replace *number* with a number from 1 through 9, and replace *sequence* with a keyboard sequence in this table.	Esc *number sequence*

Command Completion

You do not always have to remember or type the full command or option name for the CLI to recognize it. To display all possible command or option completions, type the partial command followed immediately by a question mark (?).

To complete a command or option that you have partially typed, press Tab or Spacebar. If the partially typed letters uniquely identify a command, the complete command name appears. Otherwise, a message indicates that your entry is ambiguous or invalid. Possible command completions are displayed if your entry is ambiguous.

You can also use command completion on filenames and usernames. To display all possible values, type one or more characters followed immediately by a question mark. To complete these partial entries, press Tab only. Pressing Spacebar does not work.

Online Help

The CLI provides context-sensitive help at every level of the command hierarchy. The help information tells you which commands are available at the current level in the hierarchy and provides a brief description of each.

To get help while in the CLI, type a question mark (?) in one of the following ways:

- Type a question mark at the command-line prompt. The CLI lists the available commands and options. For examples, see “CLI Operational Mode” on page 60 and “CLI Configuration Mode” on page 61.

- Type a question mark after entering the complete name of a command or command option. The CLI lists the available commands and options, then redisplays the command names and options that you typed:

```
user@host> request ?

Possible completions:
  chassis              Perform chassis-specific operations
  ipsec                Perform IP Security operations
  message              Send text message to other users
  routing-engine       Log in to Routing Engine
  security             Perform security-level operations
  services             Perform service application operations
  support              Perform JUNOS support tasks
  system               Perform system-level operations
user@host> request
```

- Type a question mark in the middle of a command name. The CLI lists possible command completions that match the letters you have entered so far, then redisplays the letters that you typed. For example, to list all operational mode commands that start with the letter **s**, type the following:

```
user@host> s?

Possible completions:
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
user@host> s
```

When you enter the help commands described in Table 28, the CLI displays usage guidelines and summary information for configuration statements and operational mode commands. You can enter help commands in operational or configuration mode.

Table 28: help Commands

CLI Command	Description
help apropos *string*	Displays help based on a text string contained in a statement or command name. If the string contains spaces, enclose it in quotation marks. You also can specify a regular expression for the string, using standard UNIX-style regular expression syntax. In configuration mode, this command displays statement names and help text that match the string specified. In operational mode, this command displays the following types of commands that match the string specified, plus help text: ■ Operational mode commands ■ help topic and help reference commands you can enter for more information For example, to get a list of statements that contain the string traps, enter the help apropos traps command in configuration mode.
help reference *string*	Displays summary information for configuration statements. For example, to display summary information for the OSPF hello interval, enter the command help reference ospf hello-interval.
help topic *string*	Displays usage guidelines for configuration statements. For example, to display usage guidelines for the OSPF hello interval, enter the command help topic ospf hello-interval.

Configuring the CLI Environment

You can configure the CLI environment for your current login session. Your settings are not retained when you exit the CLI.

To display the current CLI settings, enter the show cli command:

```
    user@host> show cli
CLI complete-on-space set to on
CLI idle-timeout disabled
CLI restart-on-upgrade set to on
CLI screen-length set to 49
CLI screen-width set to 132
CLI terminal is 'vt100'
CLI is operating in enhanced mode
CLI working directory is '/cf/var/home/remote'
```

To change the CLI environment, use the set cli operational mode command:

```
    user@host> set cli ?
Possible completions:
  complete-on-space    Set whether typing space completes current word
  directory            Set working directory
```

```
idle-timeout         Set maximum idle time before login session ends
prompt               Set CLI command prompt string
restart-on-upgrade   Set whether CLI prompts to restart after software upgrade
screen-length        Set number of lines on screen
screen-width         Set number of characters on a line
terminal             Set terminal type
```

Table 29 shows how you can change the CLI environment features.

Table 29: Configuring the CLI Environment

Environment Feature	CLI Command	Default Setting	Options
Command completion	set cli complete-on-space (on | off)	on—Pressing Tab or Spacebar completes a command.	■ Set off to allow only Tab for command completion. ■ Set on to re-enable Tab and Spacebar for command completion.
Your working directory	set cli directory *path* 8	/cf/var/home/remote	Replace *path* with the directory you want to enter when you log in to the Services Router.
Minutes of idle time	set cli idle-time *minutes*	Your session never times out unless your login class specifies a timeout.	■ To enable the timeout feature, replace *timeout* with a value between 1 and 100,000. ■ To disable the timeout feature, replace *timeout* with 0.
Your session prompt	set cli prompt *string*	*user@host* >	Replace *string* with the prompt you want. If the prompt contains spaces or special characters, enclose *string* in quotation marks (“ “).
Restart-after-upgrade prompt	set cli restart-on-upgrade (on | off)	CLI prompts you to restart the Services Router after a software upgrade.	■ Set off to disable the prompt for the session. ■ Set on to reenable the prompt.
Number of CLI output line displayed at once	set cli screen-length *length*	Variable (depends on terminal type).	■ To change the number of lines displayed on the screen, replace *length* with a value between 1 and 100,000. ■ To disable the display of a set number of lines, replace *length* with 0. (This feature can be useful when you are issuing CLI commands from scripts.)

Table 29: Configuring the CLI Environment (continued)

Environment Feature	CLI Command	Default Setting	Options
Number of CLI characters displayed on a line	set cli screen-width *width*	Variable (depends on terminal type).	To change the number of characters displayed on a line, replace *width* with a value between 0 and 100,000.
Your terminal type.	set cli terminal *terminal-type*	unknown, or set by console.	Replace *terminal-type* with one of the following values: ■ ansi ■ vt100 ■ small-xterm ■ xterm

Part 2

Installing a Services Router

- Preparing for Router Installation on page 71
- Installing and Connecting a Services Router on page 81
- Establishing Basic Connectivity on page 93
- Configuring Secure Web Access on page 115
- Configuring Autoinstallation on page 125
- Installing and Managing J-series Licenses on page 131

Chapter 5

Preparing for Router Installation

Before installing a J-series Services Router, make sure that your site has the proper operating environment and equipment. Use the checklist at the end of the chapter to help you prepare your site.

This chapter discusses the following topics:

- General Site Guidelines on page 71
- Rack Requirements on page 72
- Router Environmental Tolerances on page 73
- Fire Safety Requirements on page 73
- Power Guidelines, Requirements, and Specifications on page 74
- Network Cable Specifications on page 78
- ISDN Provisioning on page 79
- Site Preparation Checklist on page 79

General Site Guidelines

The following precautions help you plan an acceptable operating environment for your Services Router and avoid environmentally caused equipment failures:

- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow at least 6 in. (15.2 cm) of clearance between the front and back of the chassis and adjacent equipment. Ensure that there is adequate circulation in the installation location.
- Follow ESD procedures described in “Preventing Electrostatic Discharge Damage” on page 205, to avoid damaging equipment. Static discharge can cause components to fail completely or intermittently over time.
- Install blank PIM panels in empty slots, to prevent any interruption or reduction in the flow of air across internal components.

Rack Requirements

J4350 and J6350 Services Routers must be installed in a rack. Many types of racks are acceptable, including front-mount racks, four-post (telco) racks, and center-mount racks.

The following sections describe rack requirements:

- Rack Size and Strength on page 72
- Connection to Building Structure on page 73

Rack Size and Strength

The Services Router is designed for installation in a rack that complies with either of the following standards:

- A 19-in. rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronics Industry Association (http://www.eia.org)
- A 600-mm rack as defined in the four-part *Equipment Engineering (EE); European telecommunications standard for equipment practice* (document numbers ETS 300 119-1 through 119-4) published by the European Telecommunications Standards Institute (http://www.etsi.org)

  The horizontal spacing between the rails in a rack that complies with this standard is usually wider than the router's mounting ears, which measure 19 in. (48.2 cm) from outer edge to outer edge. Use approved wing devices to narrow the opening between the rails as required.

The rack rails must be spaced widely enough to accommodate the router chassis's external dimensions: 3.4 in high (8.7 cm), 17.4 in. wide (44.3 cm), and 21.1 in. (53.7 cm) deep.

The outer edges of the mounting ears extend the width of either chassis to 19 in. (48.2 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting ears. The spacing of rails and adjacent racks must also allow for the clearances around the router and rack. (See "General Site Guidelines" on page 71.)

CAUTION: If you are mounting the router in a cabinet, be sure that ventilation is sufficient to prevent overheating.

If a front-mount rack is used, we recommend supporting the back of the router with a shelf or other structure.

The J4350 and J6350 chassis height of 3.5 in. (8.7 cm) equals 2 U. Each *U* is a standard rack unit defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronics Industry Association.

Connection to Building Structure

Always secure the rack to the structure of the building. If your geographical area is subject to earthquakes, bolt the rack to the floor. For maximum stability, also secure the rack to ceiling brackets. For more information, see "Rack-Mounting Requirements and Warnings" on page 222.

Router Environmental Tolerances

Table 30 specifies the environmental conditions required for normal Services Router operation. In addition, the site must be as dust-free as possible. Dust can clog air intake vents, reducing cooling system efficiency. Check vents frequently, cleaning them as necessary.

Table 30: Router Environmental Tolerances

Description	Value
Altitude	No performance degradation to 10,000 ft (3048 m)
Relative humidity	Normal operation ensured in relative humidity range of 5% to 90%, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Non-operating storage temperature in shipping carton: –40°F (–40°C) to 158°F (70°C)
Seismic	Designed to meet Telcordia Technologies Zone 4 earthquake requirements
Maximum thermal output	■ J4350 chassis: 1092 BTU/hour (320W) ■ J6350 chassis: 1126 BTU/hour (330W)

Fire Safety Requirements

In the event of a fire emergency involving Services Routers and other network equipment, the safety of people is the primary concern. Establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire-control equipment and fire extinguishers.

In addition, establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks products must be installed in an environment suitable for electronic equipment. We recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment,

and that all local fire, safety, and electrical codes and ordinances be observed when you are installing and operating your equipment.

Fire Suppression

In the event of an electrical hazard or an electrical fire, first unplug the power cord. (For shutdown instructions, see "Powering a Services Router On and Off" on page 90.)

Then, use a Type C fire extinguisher, which uses noncorrosive fire retardants, to extinguish the fire. For more information about fire extinguishers, see "Fire Suppression Equipment" on page 74.

Fire Suppression Equipment

Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide (CO_2) and Halotron, are most effective for suppressing electrical fires. Type C fire extinguishers displace the oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, use this type of inert oxygen displacement extinguisher instead of an extinguisher that leave residues on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers) near Juniper Networks equipment. The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in minute amounts of moisture, monoammonium phosphate can become highly corrosive and corrodes most metals.

NOTE: To keep warranties effective, do not use a dry chemical fire extinguisher to control a fire at or near a Juniper Networks router. If a dry chemical fire extinguisher is used, the unit is no longer eligible for coverage under a service agreement.

Any equipment in a room in which a chemical fire extinguisher has been discharged is subject to premature failure and unreliable operation. The equipment is considered to be irreparably damaged.

We recommend that you dispose of any irreparably damaged equipment in an environmentally responsible manner.

Power Guidelines, Requirements, and Specifications

All Services Routers are available with either AC or DC power. For information about each router's power system, see "J4350 Power System" on page 21 and "J6350 Power System" on page 21.

For site wiring and power system guidelines, requirements, and specifications, see the following sections:

- Site Electrical Wiring Guidelines on page 75
- Router Power Requirements on page 76
- AC Power, Connection, and Power Cord Specifications on page 76
- DC Power, Connection, and Power Cable Specifications on page 77

Site Electrical Wiring Guidelines

WARNING: DC-powered J4350 and J6350 Services Routers are intended for installation only in a restricted access location.

When planning the electrical wiring at your site, consider the factors discussed in the following sections.

Signaling Limitations

Improperly installed wires can emit radio interference. In addition, the potential for damage from lightning strikes increases if wires exceed recommended distances, or if wires pass between buildings. The electromagnetic pulse (EMP) caused by lightning can damage unshielded conductors and destroy electronic devices. If your site has previously experienced such problems, you might want to consult experts in electrical surge suppression and shielding.

Radio Frequency Interference

You can reduce or eliminate the emission of radio frequency interference (RFI) from your site wiring by using twisted-pair cable with a good distribution of grounding conductors. If you must exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable.

Electromagnetic Compatibility

If your site is susceptible to problems with electromagnetic compatibility (EMC), particularly from lightning or radio transmitters, you might want to seek expert advice. Strong sources of electromagnetic interference (EMI) can destroy the signal drivers and receivers in the router and conduct power surges over the lines into the equipment, resulting in an electrical hazard. It is particularly important to provide a properly grounded and shielded environment and to use electrical surge-suppression devices.

CAUTION: To comply with intrabuilding lightning/surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Router Power Requirements

Table 31 lists the AC and DC power system electrical specifications for J-series Services Routers.

Table 31: AC and DC Power System Electrical Specifications

Item	Specification
AC input voltage	100 to 240 VAC nominal
AC input line frequency	50 to 60 Hz
AC system current rating	J4350 Services Routers: 6 A J6350 Services Routers: 8 A
DC input voltage	–48 to –60 VDC operating range
DC system current rating	20 A

AC Power, Connection, and Power Cord Specifications

NOTE: The AC power cord for the Services Router is intended for use with the router only and not for any other use.

Detachable AC power cords, each 2.5 m (approximately 8 ft) long, are supplied with the Services Router. The appliance coupler at the female end of the cord inserts into the appliance inlet on the faceplate of the AC power supply. The coupler is type C19 as described by International Electrotechnical Commission (IEC) standard 60320. The plug at the male end of the power cord fits into the power source receptacle that is standard for your geographical location.

NOTE: In North America, AC power cords must not exceed 4.5 m (approximately 14.75 ft) in. length, to comply with National Electrical Code (NEC) Sections 400-8 (NFPA 75, 5-2.2) and 210-52, and Canadian Electrical Code (CEC) Section 4-010(3). The cords supplied with the router are in compliance.

Table 32 lists power cord specifications and Figure 28 illustrates the plug on the AC power cord provided for each country or region.

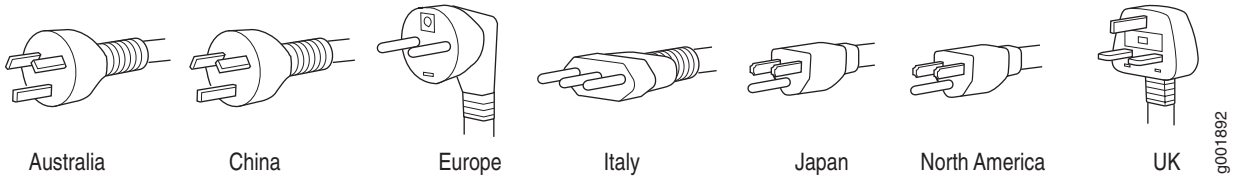
Table 32: AC Power Cord Specifications

Country	Electrical Specifications	Plug Standards
Australia	250 VAC, 10 A, 50 Hz	AS/NZ 3112–1993
China	250 VAC, 10 A, 50 Hz	GB2099.1 1996 and GB1002 1996 (CH1-10P)

Table 32: AC Power Cord Specifications (continued)

Country	Electrical Specifications	Plug Standards
Europe (except Italy and United Kingdom)	250 VAC, 10 A, 50 Hz	CEE (7) VII
Italy	250 VAC, 10 A, 50 Hz	CEI 23–16/VII
Japan	125 VAC, 12 A, 50 Hz or 60 Hz	JIS 8303
North America	125 VAC, 10 A, 60 Hz	NEMA 5-15
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363A

Figure 28: AC Plug Types



NOTE: Power cords and cables must not block access to router components or drape where people might trip on them.

For information about the AC power supply, see "J4350 Power System" on page 21 or "J6350 Power System" on page 21.

To connect the power cord during initial installation, see "Connecting Power" on page 86.

To replace the AC power cord, see "Replacing an AC Power Supply Cord" on page 159.

DC Power, Connection, and Power Cable Specifications

Each DC power supply has a single DC input (–48 VDC and return) that requires a dedicated 15 A (–48 VDC) circuit breaker. If the J6350 router contains redundant DC power supplies, one power supply must be powered by a dedicated power feed derived from feed A, and the other power supply must be powered by a dedicated power feed derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

Most sites distribute DC power through a main conduit that leads to frame-mounted DC power distribution panels, one of which might be located at the top of the rack that houses the router. A pair of cables (one input and one return) connects each set of terminal studs to the power distribution panel.

CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity.

WARNING: Power plant ground and chassis ground must be connected to the same building ground.

CAUTION: Before router installation begins, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the router (for example, by causing a short circuit).

Each DC power cable (–48 VDC and return) must be 14 AWG single-strand wire cable, or as permitted by the local code. Each lug attached to the power cables must be a ring-type, vinyl-insulated TV14-6R lug, or equivalent.

NOTE: Power cords and cables must not block access to router components or drape where people might trip on them.

For information about the DC power supply, see “J4350 Power System” on page 21 or “J6350 Power System” on page 21.

To connect the DC power cable during initial installation, see “Connecting DC Power” on page 88.

To replace a DC power cable, see “Replacing a DC Power Supply Cable” on page 162.

Network Cable Specifications

The Services Router supports interfaces that use various kinds of network cable. For information about the type of cable used by each interface, see “Network Cable Specifications and Connector Pinouts” on page 185.

ISDN Provisioning

You might need a network termination type 1 (NT1) device to connect your ISDN interface to the ISDN service. Contact your service provider for details on the following information:

- External NT1 device and ISDN cable
- If the two items are required, where to obtain the items
- List of NT1 vendors

Site Preparation Checklist

The checklist in Table 33 summarizes the tasks you need to perform when preparing a site for Services Router installation.

Table 33: Site Preparation Checklist

Item or Task	Performed By	Date	Notes
Verify that environmental factors such as temperature and humidity do not exceed router tolerances.			
Measure the distances between external power sources and the router installation site.			
Select the type of rack.			
Plan the rack location, including required space clearances.			
Secure the rack to the floor and the building structure.			
Acquire appropriate cables and connectors.			

Chapter 6

Installing and Connecting a Services Router

Make the appropriate preparations and verify the J-series equipment before installing a J-series Services Router and connecting it to a power source and the network.

This chapter contains the following topics:

- Before You Begin on page 81
- Unpacking a J-series Services Router on page 82
- Installing a J4350 and J6350 Services Router on page 83
- Connecting Interface Cables to a Services Router on page 85
- Chassis Grounding on page 86
- Connecting Power on page 86
- Powering a Services Router On and Off on page 90

Before You Begin

Before you begin installation, complete the following tasks:

- Read the information in "Maintenance and Operational Safety Guidelines and Warnings" on page 231, with particular attention to "Chassis Lifting Guidelines" on page 221.
- Determine where to install the Services Router, and verify that the rack or installation site meets the requirements described in "Preparing for Router Installation" on page 71.
- For installation, gather the following equipment and tools: mounting brackets and screws (provided), number 2 Phillips screwdriver, and mounting screws appropriate for your rack.
- To connect the router to power and ground, have ready a 14 AWG grounding cable and lug, as specified in "Chassis Grounding" on page 86, and the power

cords or cords shipped with the router. (You must supply your own power cables if you have a DC-powered router.)

NOTE: The AC power cord for the Services Router is intended for use with the router only and not for any other use.

- To connect network interfaces, have ready a length of cable used by the interface, as specified in "Network Cable Specifications and Connector Pinouts" on page 185.
- If your router has ISDN ports, you might need an NT1 device to connect to the ISDN service. For details, see "ISDN Provisioning" on page 79.

Unpacking a J-series Services Router

The Services Router is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick start instructions.

NOTE: The router is maximally protected inside the shipping carton. Do not unpack it until you are ready to begin installation.

To unpack the router:

1. Move the shipping carton to a staging area as close to the installation site as possible, but where you have enough room to remove the router.
2. Position the carton so that the arrows are pointing up.
3. Open the top flaps on the shipping carton.
4. Remove the accessory box, and verify the contents against the parts inventory on the label attached to the carton.
5. Pull out the packing material holding the router in place.
6. Verify the contents of the carton against the packing list included with the router.
7. Attach the air filter and filter cover, as shown in Figure 54.
8. Save the shipping carton and packing materials in case you later need to move or ship the router.

Installing a J4350 and J6350 Services Router

WARNING: DC-powered Services Routers are intended for installation only in a restricted access location.

You can center- or front-mount the J4350 and J6350 Services Routers in a rack. In general, a center-mount rack is preferable to a front-mount rack because the more even distribution of weight in the center-mount rack provides greater stability.

Many types of racks are acceptable, including four-post (telco) racks, enclosed cabinets, and open-frame racks. For more information about the type of rack or cabinet the J-series router can be installed into, see "Rack Requirements" on page 72.

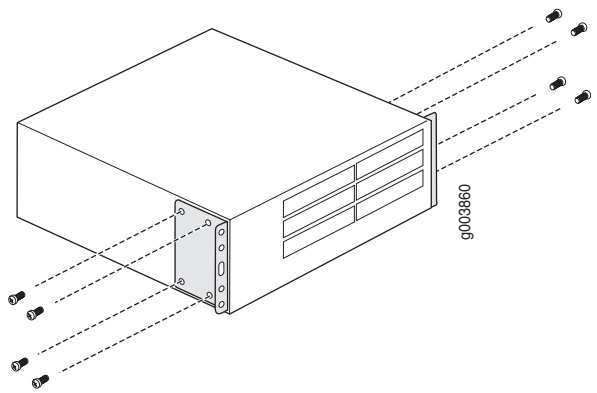
WARNING: If you are installing multiple routers in one rack, install the lowest one first and proceed upward in the rack. Install heavier routers in the lower part of the rack. The router must be mounted at the bottom of the rack if it is the only unit in the rack.

WARNING: The chassis weighs between 23 lb (10 kg) and 31 lb (14 kg). Read and follow the lifting guidelines in "Chassis Lifting Guidelines" on page 221.

To install the J4350 and J6350 router into a rack:

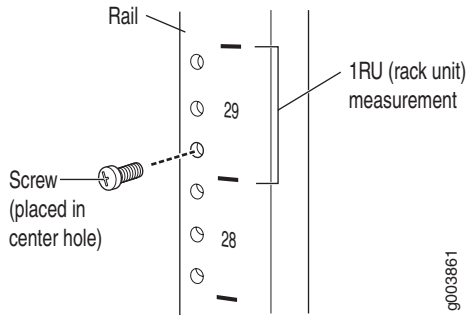
1. Attach the mounting brackets to the sides of the chassis (see Figure 29). You can position the brackets either in the center or the front. Positioning the brackets in the center offers greater stability.

Figure 29: Installing the Mounting Brackets



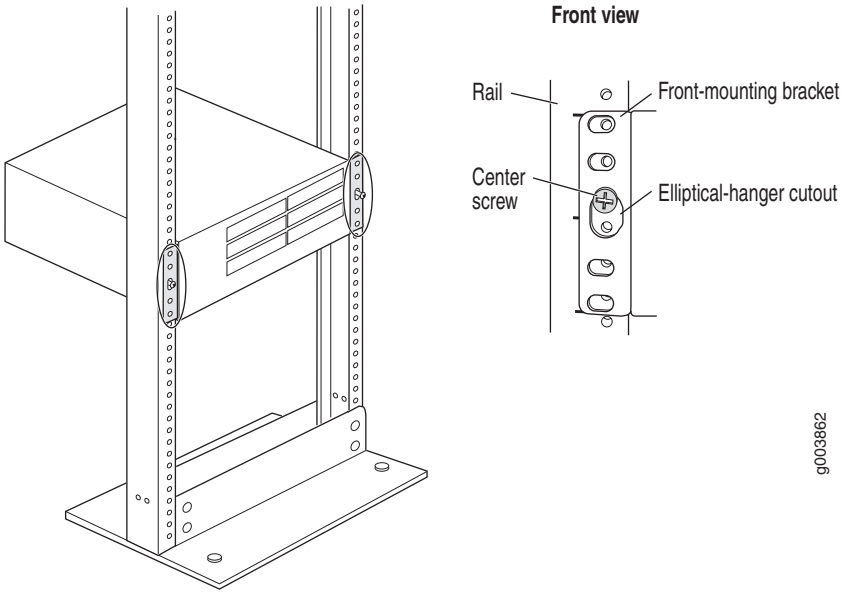
2. Attach a screw to each rack rail in the third hole down from where you want the top of the router to be positioned. Screw only part way in, leaving about ¼ in. (6 mm) distance between the screw head and the rail (see Figure 30).

Figure 30: Attaching Center Screw to the Rack



3. Lift the router and insert the larger elliptical openings in the mounting brackets onto the partially inserted screws so that the router is hanging from the two screws (see Figure 31).

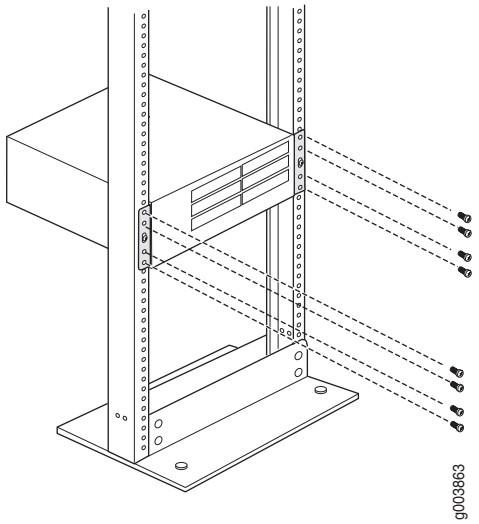
Figure 31: Hanging the Router in the Rack



4. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the router is level.

5. Install at least two mounting screws into each mounting bracket, in addition to the center screws from which the router hangs (see Figure 32). Use a number 2 Phillips screwdriver to tighten the screws.

Figure 32: Completing the Installation



Connecting Interface Cables to a Services Router

You connect the interfaces installed in the Services Router to various network media. For more information about the network interfaces supported on the router, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

1. Have ready a length of the type of cable used by the interface, as specified in "Network Cable Specifications and Connector Pinouts" on page 185.

2. Insert the cable connector into the cable connector port on the interface faceplate.

3. Arrange the cable as follows to prevent it from dislodging or developing stress points:

   a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.

   b. Place excess cable out of the way in a neatly coiled loop.

   c. Place fasteners on the loop to help maintain its shape.

Chassis Grounding

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the Services Router must be adequately grounded before power is connected. In addition to the grounding pin on the AC power plug cord, a threaded insert (PEM nut), screw, and washer are provided on the rear of the chassis to connect the router to earth ground.

CAUTION: Before router installation begins, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the router (for example, by causing a short circuit).

The grounding cables must be 14 AWG single-strand wire cable, and must be able to handle amperage up to 20 A.

Each grounding lug must be a ring-type, vinyl-insulated TV14-6R lug, or equivalent, to accommodate the 14 AWG cable.

To ground the router before connecting power, you connect the grounding cable to earth ground and then attach the lug on the cable to the chassis grounding point, with the screw. (See “Connecting Power” on page 86.)

Connecting Power

J4350 Services Routers have a single fixed power supply. J6350 Services Routers have one or two field-replaceable power supplies. For more information about the J-series power specifications, see “Power Guidelines, Requirements, and Specifications” on page 74.

WARNING: DC-powered Services Routers are intended for installation only in a restricted access location.

Connecting AC Power

The router must be connected to earth ground during normal operation. The protective earthing terminal on the rear of the chassis is provided to connect the router to ground. Additional grounding is provided to an AC-powered router when you plug its power supply into a grounded AC power receptacle.

The AC power cord shipped with the router connects the router to earth ground when plugged into an AC grounding-type power outlet. The router must be connected to earth ground during normal operation.

For power cord requirements, see “AC Power, Connection, and Power Cord Specifications” on page 76

To connect AC power to the router:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strip to the ESD point on the chassis. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.

2. Use a grounding cable to connect the router to earth ground: (For cable requirements, see “Chassis Grounding” on page 86.)

   a. Verify that a licensed electrician has attached an appropriate grounding cable lug to the grounding cable.

   b. Connect one end of the grounding cable to a proper earth ground, such as the rack in which the router is installed.

   c. With a Phillips screwdriver, remove the screws and washers from the PEM nuts at the grounding point on the rear of the chassis.

   d. Place the grounding lug at the other end of the cable over the grounding point, as shown in Figure 33.

   e. Secure the cable lug to the grounding point, first with the washers, then with the screws.

3. Locate the power cord or cords shipped with the router, which has a plug appropriate for your geographical location. For power cord specifications, see “Power Guidelines, Requirements, and Specifications” on page 74.

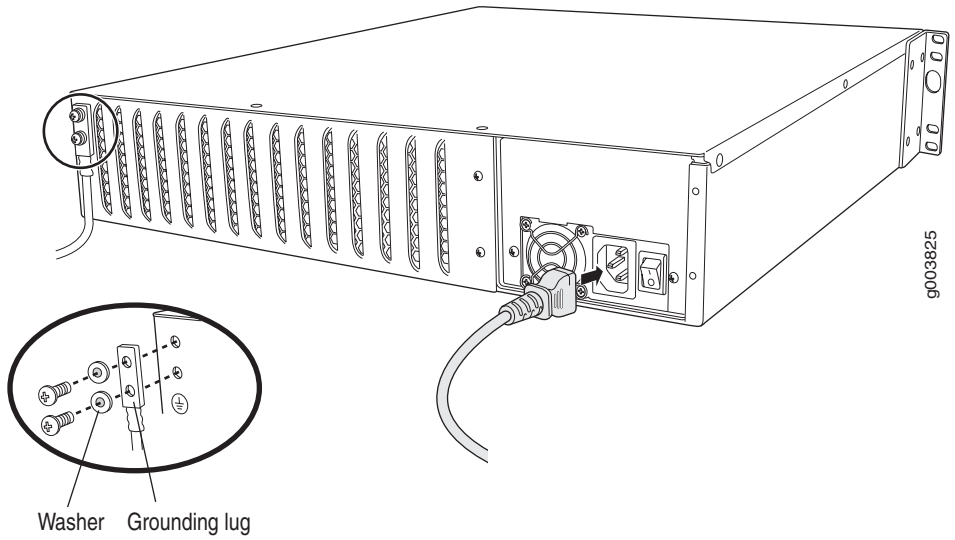
4. For each power supply:

   a. Insert the appliance coupler end of a power cord into the appliance inlet on the power supply faceplate, as shown in Figure 33.

   b. Insert the plug into an AC power source receptacle.

5. Verify that the power cord does not block access to router components or drape where people can trip on it.

Figure 33: Connecting AC Power to the J4350 or J6350 Services Router



Connecting DC Power

CAUTION: If your J6350 Services Router includes an optional redundant DC power supply, connect each of the two power supplies to different input power sources. Failure to do so makes the router susceptible to total power failure if one of the power supplies fails.

The router must be connected to earth ground during normal operation. The protective earthing terminal on the rear of the chassis is provided to connect the router to ground.

For DC cable requirements, see "DC Power, Connection, and Power Cable Specifications" on page 77.

To connect DC power to the router:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strip to the ESD point on the chassis. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
2. Use a grounding cable to connect the router to earth ground: (For cable requirements, see "Chassis Grounding" on page 86.)
   a. Verify that a licensed electrician has attached an appropriate grounding cable lug to the grounding cable.
   b. Connect one end of the grounding cable to a proper earth ground, such as the rack in which the router is installed.

c. With a Phillips screwdriver, remove the screws and washers from the PEM nuts at the grounding point on the rear of the chassis.

d. Place the grounding lug at the other end of the cable over the grounding point, as shown in Figure 34.

e. Secure the cable lug to the grounding point, first with the washers, then with the screws.

NOTE: A DC power supply in a Services Router becomes grounded when you connect a grounding cable between the router and earth ground.

---

3. For each power supply:

   a. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.

CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity.

---

   b. Verify that a licensed electrician has attached the appropriate power cable lugs to the negative and positive DC source power cables.

   c. Use a Phillips screwdriver to remove the clear plastic cover protecting the terminal block.

   d. Within the terminal block, remove the two center screws next to the labels –48 VDC and RTN.

      Each screw contains a captive washer to secure a DC source power cable lug to the terminal block.

   e. Using one of the removed screws, secure the positive (+) DC source power cable lug to the RTN terminal. Tighten the screw until snug. Do not overtighten. Apply between 8 lb-in. (0.9 Nm) and 9 lb-in. (1.02 Nm) of torque to the screw.

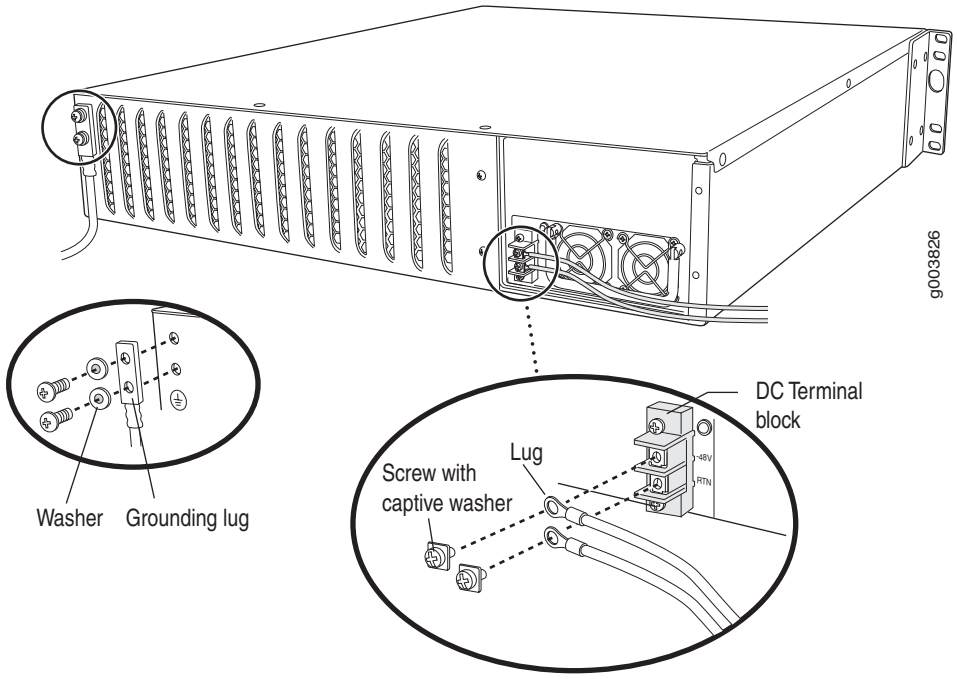
   f. Using the other removed screw, secure the negative (–) DC source power cable lug to the –48 VDC terminal. Tighten the screw until snug. Do not overtighten. Apply between 8 lb-in. (0.9 Nm) and 9 lb-in. (1.02 Nm) of torque to the screw.

   g. Dress the power cables appropriately.

h. Replace the clear plastic cover over the terminal block.

4. Verify that the power cables do not block access to router components or drape where people can trip on them.

Figure 34: Connecting DC Power to the J4350 or J6350 Services Router



Powering a Services Router On and Off

To power on a Services Router, press the power button. The Routing Engine boots as the power supply completes its startup sequence. The POWER LED lights during startup and remains on steadily when the router is operating normally.

To power off a Services Router, you can shut it down in one of the following ways:

- Graceful shutdown—Press and release the power button. The router begins gracefully shutting down the operating system and then powers itself off.
- Immediate shutdown—Press the power button and hold it for more than 5 seconds. The router immediately powers itself off without shutting down the operating system.

To remove power completely from the router, unplug the AC power cord or switch off the DC power source. The power button on the Services Router is a standby power switch. If the router is connected to a power source when you press the

power button to power the router off, the router remains in standby mode and a small amount (5 V and 3.3 V) of standby voltage is still available in the chassis.

Chapter 7

Establishing Basic Connectivity

The JUNOS software is preinstalled on the Services Router. When the router is powered on, it is ready to be configured. If the router does not have a configuration from the factory or your service provider, you must configure the software to establish basic connectivity.

If you are setting up a Services Router for the first time, you can use either J-Web Quick Configuration or a configuration editor to configure basic connectivity. For a brief explanation of J-Web Quick Configuration and the J-Web and CLI configuration editors, see "Services Router User Interface Overview" on page 49.

If you are setting up many Services Routers, autoinstallation can help automate the configuration process. For more information about autoinstallation, see "Configuring Autoinstallation" on page 125.

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

- Basic Connectivity Terms on page 93
- Basic Connectivity Overview on page 94
- Before You Begin on page 98
- Connecting to a Services Router on page 99
- Configuring Basic Settings with J-Web Quick Configuration on page 105
- Configuring Basic Settings with a Configuration Editor on page 108
- Verifying Basic Connectivity on page 113

Basic Connectivity Terms

Before configuring basic connectivity, become familiar with the terms defined in Table 34.

Table 34: Basic Connectivity Terms

Term	Definition
domain name	Name that identifies the network or subnetwork of a router.
Dynamic Host Configuration Protocol (DHCP)	Protocol for assigning dynamic IP addresses to devices on a network.
gateway	Packets destined for IP addresses not identified in the routing table are sent to the default gateway.
hostname	Unique name that identifies a router on the network.
loopback address	IP address of a Services Router on logical interface lo0.0 that is always active and available to external hosts and as the source address for outgoing packets.
Network Time Protocol (NTP)	Protocol that provides a reliable way of synchronizing the system time of a router.
root user	A superuser or system administrator who can perform any task in the file system.
secure shell (SSH)	Protocol that provides a secured method of logging in to a remote network system.
Telnet	Software that allows a computer to act as a remote terminal on a network system.

Basic Connectivity Overview

To connect your Services Router to the network and establish basic connectivity, you enter information about your network. This overview contains the following topics:

- Router Identification on page 95
- Root Password on page 95
- Time Zone and System Time on page 95
- Network Settings on page 96
- Default Gateway on page 96
- Backup Router on page 96
- Loopback Address on page 96
- Built–In Ethernet Interface Address on page 97
- Management Access on page 97

Router Identification

The domain name defines the network or subnetwork that the Services Router belongs to. The hostname refers to the specific machine, while the domain name is shared among all the devices in a given network. Together the hostname and domain name identify the router in the network.

Root Password

The root user has complete privileges to configure the Services Router, and manage files in the router's file system. Initially, the root password is not defined on the router. To ensure basic security, you must define the root password during initial configuration. If a root password is not defined, you cannot commit configuration settings to take effect on the router.

If you use a plain-text password, the router displays the password as a encrypted string so that users viewing the configuration cannot easily see the password.

The root password must meet the following conditions:

- The password must be at least 6 characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.
- Valid passwords must contain at least one change of case or character class.

For Common Criteria environments only, the password must be between 10 and 20 characters long and must include at least three of the five character classes (uppercase letters, lowercase letters, punctuation marks, numbers, and other special characters). Control characters are not recommended. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

Time Zone and System Time

You define the time zone for the location where you plan to operate the Services Router by using a designation that consists of the following information for the location:

- Name of the continent or ocean—For example, America or Atlantic
- Name of the major city or other geographic feature in the time zone—For example, Detroit or Azores

A Network Time Protocol (NTP) server provides accurate time across a network. The router synchronizes the system time with the NTP server, and periodically accesses the NTP server to maintain the correct time.

The time zone and system time must be accurate so that the router schedules events and operations as expected.

For Common Criteria compliance, you must configure NTP to provide accurate timestamps for system log messages. For more information, see the *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*.

Network Settings

A Domain Name System (DNS) server on the network maintains a database for resolving hostnames and IP addresses. Network devices can query the DNS server by hostnames rather than IP addresses. The router accesses the DNS servers that are added to the configuration to resolve hostnames in the order in which you list them.

If you plan to include your router in several domains, you can add these domains to the configuration so that they are included in a DNS search. When DNS searches are requested, the domain suffixes are appended to the hostnames.

Default Gateway

A default gateway is a static route that is used to direct packets addressed to networks not explicitly listed in the routing table. If a packet arrives at the Services Router with an address that the router does not have routing information for, the router sends the packet to the default gateway. The default gateway entry is always present in the routing and forwarding tables.

Backup Router

You can specify a backup router to take over when the routing protocol process of the Services Router is not running, usually when the Services Router is booting, or if its routing protocol process has failed. Packets arriving at a Services Router in this situation are routed to the backup router. When the routing protocol process starts up again, the address of the backup router is removed from the routing and forwarding tables of the Services Router. The backup router must be located on the same subnet.

NOTE: To configure a backup router, you must use the CLI or J-Web configuration editor. You cannot configure a backup router with J-Web Quick Configuration.

Loopback Address

The loopback address is the IP address of the Services Router. The loopback address ensures that the Services Router provides an IP address to management applications. Because it must always be available to hosts attempting to route packets to the Services Router, the loopback address resides on an interface that is always active, known as the loopback interface (lo0.0). Setting a loopback address ensures that the Services Router can receive packets addressed to the loopback address as long as the router is reachable though any entry (ingress) interface. In addition, applications such as NTP, RADIUS, and TACACS+ can use the loopback address as the source address for outgoing packets.

If you use the J-Web Set Up Quick Configuration page, you can either set a loopback address of your choice or have the loopback address automatically set to 127.0.0.1 when you click **Apply** or **OK** to commit the configuration.

Built–In Ethernet Interface Address

The built-in Gigabit Ethernet interfaces, ge-0/0/0 through ge-0/0/3, on the front panel of the Services Router, are the interfaces through which you perform initial router setup. The examples in this guide use the ge-0/0/0 interface as the management interface, but you can use any built-in Ethernet port for management. After the initial configuration is complete, you can attach the built-in Ethernet port that you are using for management purposes to the management network.

Before initial configuration, when the factory default configuration is active, the Services Router attempts to perform autoinstallation by obtaining a router configuration through all its connected interfaces, including ge-0/0/0. The Services Router acts as a DHCP client out the built-in Ethernet interfaces.

If the Services Router does not find a DHCP server within a few seconds, it sets the address of ge-0/0/0 to 192.168.1.1/24 and becomes a DHCP server out the ge-0/0/0 interface.

NOTE: If the ge-0/0/1 interface is being used, it is set to 192.168.2.1/24.

With the router temporarily acting as a DHCP server, you can manually configure it with the J-Web interface. Any DHCP client host, for example, a PC or laptop computer, directly connected to ge-0/0/0 receives an address on the 192.168.1.1/24 network.

NOTE: The DHCP functionality for initial setup is different from the configurable DHCP server functionality of the Services Router during operation. To configure the Services Router as a DHCP server, see the *J-series Services Router Administration Guide*.

Once you connect your laptop or PC to ge-0/0/0, you can use a Web browser to visit the address 192.168.1.1/24, access the J-Web Set Up Quick Configuration page, and complete the initial configuration of the router.

After you perform the initial configuration and commit it by clicking **Apply** or **OK** on the Set Up page, the configured router can no longer act as a DHCP server. Therefore, in order to continue using it as a management interface you should configure the IP address of the interface as part of the initial configuration.

Management Access

Telnet allows you to connect to the Services Router and access the CLI to execute commands from a remote system. Telnet connections are not encrypted and therefore can be intercepted.

Telnet access to the root user is prohibited. You must use more secure methods, such as SSH, to log in as root.

If you are using a JUNOScript server to configure and monitor routers, you can activate clear-text access on the router to allow unencrypted text to be sent directly over a TCP connection without using any additional protocol (such as SSH, SSL, or Telnet). Information sent in clear text is not encrypted and therefore can be intercepted. For more information about the JUNOScript application programming interface (API), see the *JUNOScript API Guide*.

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

SSH also allows you to connect to the router and access the CLI to execute commands from a remote system. However, unlike Telnet, SSH encrypts traffic so that it cannot be intercepted.

SSH can be configured so that connections are authenticated by a digital certificate. SSH uses public-private key technology for both connection and authentication. The SSH client software must be installed on the machine where the client application runs. If the SSH private key is encrypted (for greater security), the SSH client must be able to access the passphrase used to decrypt the key.

For information about obtaining SSH software, see http://www.ssh.com and http://www.openssh.com.

Before You Begin

Before you begin initial configuration, complete the following tasks:

- Install the Services Router in its permanent location, as described in “Installing and Connecting a Services Router” on page 81.
- Gather the following information:
  - Hostname for the router on the network
  - Domain that the router belongs to on the network
  - Password for the root user
  - Time zone where the router is located
  - IP address of an NTP server (if NTP is used to set the time on the router)
  - IP address of a DNS server
  - List of domains that can be appended to hostnames for DNS resolution
  - IP address of the default gateway

- IP address to be used for the loopback interface
- IP address of the built-in Ethernet interface that you will use for management purposes. The examples in this guide use the ge-0/0/0 interface.

- If you are performing the initial configuration with the J-Web interface, collect the following equipment:
  - A management device, such as a laptop, with an Ethernet port
  - An Ethernet cable
- If you are performing the initial configuration with the CLI, collect the following equipment:
  - A management device, such as a PC or laptop, with a serial port and an asynchronous terminal application (such as Microsoft Windows Hyperterminal)
  - An RJ-45 to DB-9 serial port adapter (provided)
  - A Ethernet cable (provided)
  - For a remote connection, two dial-up modems
  - For a remote modem connection, a DB-9 female to DB-25 male adapter, or other adapter appropriate for your modem (not provided)

Connecting to a Services Router

You can connect to the Services Router using the J-Web or CLI interface.

This section contains the following topics:

- Connecting to the J-Web Interface on page 99
- Connecting to the CLI Locally on page 101
- Connecting to the CLI Remotely on page 103

Connecting to the J-Web Interface

If you plan to use the J-Web interface to configure the Services Router, you must connect through one of the built-in Ethernet management ports, as shown in Figure 35.

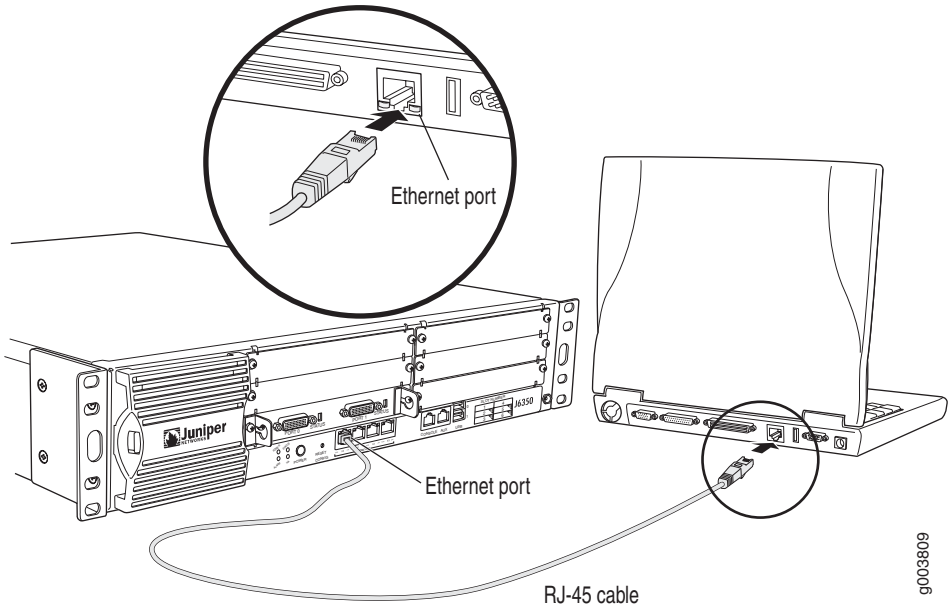
When the Services Router is powered on for the first time, the system looks for a DHCP server, and if it does not find one, it assigns an IP address within the 192.168.1.0/24 subnetwork to any devices connected to it.

To connect to the J-Web interface through port 0 on the router (see Figure 35):

1. On the management device, such as a PC or laptop, you use to access the J-Web interface, verify that the address of the port that you connect to the router is set to one of the following:
   - An Ethernet address on the 192.168.1/24 subnetwork other than 192.168.1.1
   - An Ethernet address from a DHCP server
2. Turn off the power to the management device.
3. Plug one end of the Ethernet cable into the Ethernet port on the management device.
4. Connect the other end of the Ethernet cable to the built-in Ethernet port on the router.
5. Power on the router by pressing the power button on the front panel.
6. Wait until the STATUS LED on the front panel turns solid green.
7. Turn on the power to the management device. The router assigns an IP address to the management device within the 192.168.1.0/24 subnetwork if the device is configured to use DHCP.
8. From the management device, open a Web browser and enter the IP address 192.168.1.1 in the address field. The Set Up Quick Configuration page appears.
9. Configure basic settings for your router as described in “Configuring Basic Settings with J-Web Quick Configuration” on page 105.

NOTE: You must manually configure the IP address for the management port you are using before you save your initial configuration. When you save the configuration for the first time, you will lose the connection to the router if you have not manually configured the IP address. If you lose connection through the management interface, you must connect through the console port.

Figure 35: Connecting to the Gigabit Ethernet Port on the Services Router



Connecting to the CLI Locally

If you plan to use the CLI to configure the router, you must connect through the console port, as shown in Figure 36.

NOTE: Figure 36 show a connection to a local management device. A remote connection to the router through a modem requires the cable and connector shown (provided in the router's accessory box), plus a DB-9 female to DB-25 male (or similar) adapter for your modem, which you must purchase separately.

To connect to the CLI using a local management device through the console port on the router:

1. Turn off power to the router.
2. Turn off the power to the management device, such as a PC or laptop computer, that you are using to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with your router into the RJ-45 to DB-9 serial port adapter supplied with your router (see Figure 36).
4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see Figure 36).
5. Connect the other end of the Ethernet rollover cable to the console port on the router (Figure 36).

6. Turn on the power to the management device.

7. Start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

8. Configure the port settings as follows:

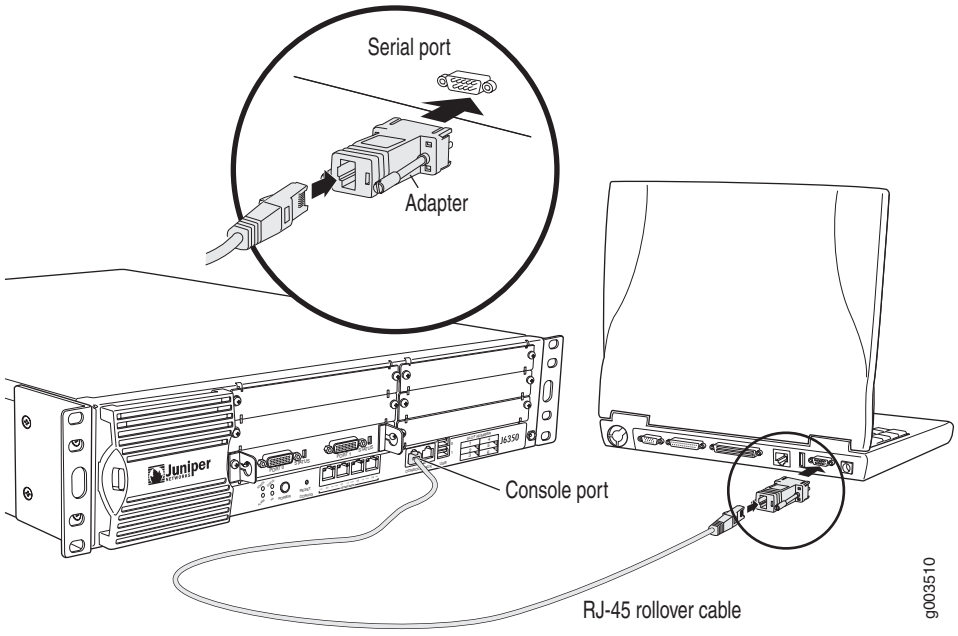
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

9. Power on the router by pressing the power button on the front panel. Verify that the POWER LED on the front panel turns green.

   The terminal emulation screen on your management device displays the boot sequence. When the router has finished booting, a login prompt appears.

10. Log in as the user "root". No password is required at initial connection, but you must assign a root password before committing any configuration settings.

Figure 36: Connecting to the Console Port on the Services Router



Connecting to the CLI Remotely

You can connect to the CLI from a remote location through two dial-up modems: a modem that is connected to the console port on the Services Router and a second modem connected to a remote management device. The modem connection allows you to remotely perform the same console operations you can perform locally.

This section contains the following topics:

- Configuring the Modem at the Router End on page 103
- Connecting the Modem to the Console Port on page 104
- Connecting to the CLI at the User End on page 104

Configuring the Modem at the Router End

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

Before you can connect a dial-up modem to the console port on the Services Router, you must configure the modem to accept a call on the first ring and accept Data Terminal Ready (DTR) signals. You must also disable flow control on the modem.

To configure the modem on the router end:

1. Connect the modem to a PC or laptop computer.
2. Power on the modem.
3. From the PC or laptop computer, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the COM port to which the modem is connected (for example, COM1).
4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
5. In the HyperTerminal window, enter AT.

   An OK response verifies that the modem communicates successfully with the COM port on the PC or laptop.

6. To configure the modem to answer a call on the first ring, enter ATS0=1.
7. To configure the modem to accept modem control Data Terminal Ready (DTR) signals, enter AT&D1.
8. To disable flow control, enter AT&K0.
9. To save modem settings, enter AT&W.

Connecting the Modem to the Console Port

NOTE: Most modems have an RS-232 DB-25 connector. You must separately purchase an adapter to connect your modem to the RJ-45 to DB-9 adapter and Ethernet cable supplied with the router.

To connect the dial-up modem to the console port on the router:

1. Turn off power to the router.
2. Turn off the power to the modem.
3. Plug one end of the Ethernet rollover cable supplied with your router into the console port on the router.
4. Plug the other end of the Ethernet rollover cable into the RJ-45 to DB-9 serial port adapter supplied with your router.
5. Connect the serial port adapter to a separately purchased DB-9 female to DB-25 male adapter, or other adapter appropriate for your modem.
6. Plug the modem adapter into the DB-25 connector on the modem.
7. Connect the modem to your telephone network.
8. Turn on the power to the modem.
9. Power on the router by pressing the power button on the front panel. Verify that the POWER LED on the front panel turns green.

Connecting to the CLI at the User End

To remotely connect to the CLI through a dial-up modem connected to the console port on the router:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.
2. On the PC or laptop computer, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal).

3. Select the COM port to which the modem is connected (for example, COM1).

4. Configure the port settings as follows:

   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. In the HyperTerminal window, enter AT.

   An OK response verifies that the modem communicates successfully with the COM port on the PC or laptop.

6. To dial the modem that is connected to the console port on the router, enter ATDT *remote-modem-number*. For example, if the number of the modem connected to the console port on the router is 0013033033030, enter ATDT 0013033033030.

   The router login prompt appears.

7. Log in as the user "root". No password is required at initial connection, but you must assign a root password before committing any configuration settings.

Configuring Basic Settings with J-Web Quick Configuration

J-Web Quick Configuration allows you to configure basic settings. Figure 25 shows the Quick Configuration page for basic setup.

Before you configure the router, gather the information described in "Before You Begin" on page 98.

To configure basic settings with J-Web Quick Configuration:

1. If you have not already done so, connect a management device to the ge-0/0/0 interface on port 0/0. For instructions, see "Connecting to the J-Web Interface" on page 99.

2. If the Set Up Quick Configuration page is not displayed, select **Configuration > Quick Configuration > Set Up**.

3. Enter information into the Set Up Quick Configuration page, as described in Table 35.

4. Click one of the following buttons:

   - To apply the configuration and stay in the Set Up Quick Configuration page, click **Apply**.

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

NOTE: After initial configuration is complete, the Services Router stops functioning as a DHCP server. If you change the IP address of ge-0/0/0 and have the management device configured to use DHCP, you lose your DHCP lease and your connection to the router through the J-Web interface. To reestablish a connection, either set the IP address on the management device manually, or connect ge-0/0/0 to the management network and access the router another way—for example, through the console port.

5. To check the configuration, see "Displaying Basic Connectivity Configurations" on page 113.

Table 35: Set Up Quick Configuration Summary

Field	Function	Your Action
Identification		
Host Name (required)	Defines the hostname of the router.	Type the hostname.
Domain Name	Defines the network or subnetwork that the machine belongs to.	Type the domain name.
Root Password (required)	Sets the root password that user "root" can use to log in to the router.	Type a plain-text password that the system encrypts. **NOTE:** After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.
Verify Root Password (required)	Verifies the root password has been typed correctly.	Retype the password.
Time		
Time Zone	Identifies the time zone that the router is located in.	From the list, select the appropriate time zone.
NTP Servers	Specify an NTP server that the router can reach to synchronize the system time.	To add an IP address, type it in the box to the left of the Add button, then click **Add**. To delete an IP address, click on it in the box above the Add button, then click **Delete**.

Table 35: Set Up Quick Configuration Summary (continued)

Field	Function	Your Action
Current System Time	Synchronizes the system time with the NTP server, or manually set the system time and date.	■ To immediately set the time using the NTP server, click **Set Time via NTP**. The router sends a request to the NTP server and synchronizes the system time. **NOTE:** If you are configuring other settings on this page, the router also synchronizes the system time using the NTP server when you click **Apply** or **OK**. ■ To set the time manually, click **Set Time Manually**. A pop-up window allows you to select the current date and time from lists.
Network		
DNS Name Servers	Specify a DNS server that the router can use to resolve hostnames into addresses.	To add an IP address, type it in the box to the left of the Add button, then click **Add**. To delete an IP address, click on it in the box above the Add button, then click **Delete**.
Domain Search	Adds each domain name that the router is included in to the configuration so that they are included in a DNS search.	To add a domain name, type it in the box to the left of the Add button, then click **Add**. To delete a domain name, click on it in the box above the Add button, then click **Delete**.
Default Gateway	Defines a default gateway through which to direct packets addressed to networks not explicitly listed in the routing table.	Type a 32-bit IP address, in dotted decimal notation.
Loopback Address	Defines a reserved IP address that is always available on the router. If no address is entered, this address is set to 127.0.0.1/32.	Type a 32-bit IP address and prefix length, in dotted decimal notation.
ge-0/0/0 Address	Defines the IP address and prefix length of ge-0/0/0. The interface ge-0/0/0 is typically used as the management interface for accessing the router. The DHCP client sets this address to 192.168.1.1/24 if no DHCP server is found.	Type a 32-bit IP address and prefix length, in dotted decimal notation. **NOTE:** You must enter the ge-0/0/0 address on the Quick Configuration Set Up page before you click **Apply** or **OK**. If you do not manually configure this address, you will lose your connection to the J-Web interface when you click **Apply** or **OK**.
Management Access		
Allow Telnet Access	Allows remote access to the router using Telnet.	To enable Telnet access, select the check box.

Table 35: Set Up Quick Configuration Summary (continued)

Field	Function	Your Action
Allow JUNOScript over Clear-Text Access	Allows JUNOScript to access the router using a protocol for sending unencrypted text over a TCP connection.	To enable JUNOScript access over clear text, select the check box.
Allow SSH Access	Allows remote access to the router using SSH.	To enable SSH access, select the check box.

Configuring Basic Settings with a Configuration Editor

To establish basic connectivity on a Services Router, you identify the router, connect the router to the network, and specify basic network settings.

In a typical network, the Services Router has the basic settings listed in Table 36. Determine the values to set on the Services Router in your network.

Table 36: Sample Settings on a Services Router

Services Router Property	Sample Value
Services Router hostname	routera
Access for user "root"	SSH RSA public key
IP address of the NTP server used to synchronize system time on the Services Router	10.148.2.21
Services Router location	Sunnyvale, California, USA, which is in the America/Los_Angeles time zone
IP address of the DNS server to which DNS requests are sent	10.148.2.32
Domains to which the Services Router belongs	lab.router.net and router.net
IP address of a backup router to use while the Services Router is booting or if the routing protocol processes fail to start	192.168.2.12/24
Loopback IP address and prefix length for the Services Router lo0 interface	172.16.1.24/32
IP address and prefix length for the Services Router ge-0/0/0 interface	192.168.1.1/24

You can configure basic settings in the J-Web interface from a device attached to the ge-0/0/0 interface on port 0. For instructions, see "Connecting to the J-Web Interface" on page 99. You can also connect to the CLI to configure basic settings. For instructions, see "Connecting to the CLI Locally" on page 101 and "Connecting to the CLI Remotely" on page 103.

To use a configuration editor to configure basic settings:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure basic settings, perform the configuration tasks described in Table 37.
3. If you are using the J-Web interface, click **Commit** to view a summary of your changes, then click **OK** to commit the configuration. If you are using the CLI, commit the configuration by entering the commit command.
4. To check the configuration, see "Displaying Basic Connectivity Configurations" on page 113.

Table 37: Configuring Basic Settings

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to System, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit system
Define the hostname of the router.	In the Host name box, type the hostname of the router—for example, routera.	Set the hostname. For example: set host-name routera
Name the domain in which the router is located.	In the Domain name box, type the domain name of the router—for example, lab.router.net.	Set the domain name. For example: set domain-name lab.router.net
Allow SSH remote access.	1. In the Nested configuration section, next to Services, click **Configure** or **Edit**. 2. Next to Ssh, click **Configure** or **Edit**. 3. Click **OK**. 4. Click **OK** a second time to return to the System level in the configuration editor hierarchy.	Set remote access for SSH: set services ssh

Table 37: Configuring Basic Settings (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Define root authentication for access to the router. **NOTE:** For readability, the entire key is not shown.	1. In the Nested configuration section, next to Root authentication, click **Configure** or **Edit**. 2. Next to Ssh rsa, click **Add New Entry**. 3. In the Authorized key box, type the RSA password—for example, ssh-rsa AAAAB3Nza...D9Y2gXF9ac== root@routera.lab.router.net 4. Click **OK**. 5. Click **OK** a second time to return to the System level in the configuration editor hierarchy.	Set the root password. For example: set root-authentication ssh-rsa "ssh-rsa AAAAB3Nza...D9Y2gXF9ac== root@routera.lab.router.net"
Define the time zone the router is located in.	In the Time zone list, select the time zone for your router—for example, **America/Los_Angeles**.	Set the time zone. For example: set time-zone America/Los_Angeles
Define the NTP server that NTP requests can be sent to.	1. In the Nested configuration section, next to Ntp, click **Configure** or **Edit**. 2. Next to Server, click **Add New Entry**. 3. In the Address box, type the NTP server's IP address—for example, 10.148.2.21 4. Click **OK**. 5. Click **OK** a second time to return to the System level in the configuration editor hierarchy.	Set the address of the NTP server. For example: set ntp server 10.148.2.21
Define the DNS server that receives DNS requests.	1. Next to Name server, click **Add New Entry**. 2. In the Address box, type the address of the DNS server—for example, 10.148.2.32. 3. Click **OK**.	Set the address of the DNS server. For example: set name-server 10.148.2.32

Table 37: Configuring Basic Settings (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Add each domain that the router belongs to.	1. Next to Domain search, click **Add New Entry**. 2. In the Value box, type the name of the domain in which the router is located—for example, lab.router.net. 3. Click **OK**. 4. Next to Domain search, click **Add New Entry**. 5. In the Value box, type the name of another domain that the router belongs to—for example, router.net. 6. Click **OK**.	Set the domains to be searched. For example: set domain-search lab.router.net set domain-search router.net
Define the backup router to be used when the router is booting or the routing protocol processes are not running.	In the Backup router section, next to Address, type the IP address of the backup router—for example, 192.168.2.44.	Set the address for the backup router. For example: set backup router address 192.168.2.44

Table 37: Configuring Basic Settings (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Define the IP address for lo0.0.	1. In the configuration editor hierarchy, next to Interfaces, click **Configure** or **Edit**. 2. In the Interface table, locate the lo0 row and click **Unit**. 3. In the Unit table, click **0**, and in the Family section next to Inet, click **Configure** or **Edit**. 4. To delete the existing IP address, click the **Discard** button. Select the **Delete Configuration Below This Point** option button from the next display. 5. Next to Address, click **Add new entry**. 6. In the Source box, type the address and prefix length for the loopback interface—for example, 172.16.1.24/32. 7. Click **OK**.	1. From the [edit] hierarchy level, enter edit interfaces 2. Delete the existing IP address: delete lo0 unit 0 family inet address 3. Set the IP address and prefix length of lo0.0. For example: set lo0 unit 0 family inet address 172.16.1.24/32
Define the IP address for ge-0/0/0.	1. In the configuration editor hierarchy, next to Interfaces, click **Configure** or **Edit**. 2. In the Interface table, locate the ge-0/0/0 row and click **Unit**. 3. In the Unit table, click **0**, and in the Family section next to Inet, click **Configure** or **Edit**. 4. To delete the existing IP address, click the **Discard** button. Select the **Delete Configuration Below This Point** option button from the next display. 5. Next to Address, click **Add new entry**. 6. In the Source box, type the address and prefix length for the management interface—for example, 192.168.1.1/24. 7. Click **OK**.	1. Delete the existing IP address: delete ge-0/0/0 unit 0 family inet address. 2. Set the IP address and prefix length of ge-0/0/0. For example: set ge-0/0/0 unit 0 family inet address 192.168.1.1/24

Verifying Basic Connectivity

To verify that the Services Router has the settings you configured, perform the following task.

Displaying Basic Connectivity Configurations

Purpose Verify the configuration of basic connectivity. Because the basic connectivity settings appear in different places in the configuration hierarchy, displaying the entire configuration at once makes viewing the settings easier.

Action From the J-Web interface, select **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the show command. The following sample output displays the sample values configured in Table 37. Your output displays the values you set.

Sample Output

```
system {
    host-name routera;
    domain-name lab.router.net;
    domain-search [ lab.router.net router.net ];
    backup-router 192.168.2.44;
    time-zone America/Los_Angeles;
    root-authentication {
        ssh-rsa "ssh-rsa AAAAB3Nza...D9Y2gXF9ac==root@routera.lab.router.net";
    }
    name-server {
        10.148.2.32;
    }
    services {
    }
    ntp {
        server 10.148.2.21;
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.24/32;
            }
        }
    }
}
```

What It Means The output shows the configuration of basic connectivity. Verify that the values displayed are correct for your Services Router. For more information about the format of a configuration file, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Chapter 8

Configuring Secure Web Access

You can manage a Services Router remotely through the J-Web interface. To communicate with the Services Router, the J-Web interface uses Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the router by means of HTTP is vulnerable to interception and attack. To enable secure Web access, a Services Router supports Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

You can use J-Web Quick Configuration, the J-Web configuration editor, or the CLI configuration editor to configure secure Web access.

This chapter contains the following topics. For more information about the J-Web interface, see the *J-Web Interface User Guide*.

- Secure Web Access Terms on page 115
- Secure Web Access Overview on page 116
- Before You Begin on page 117
- Configuring Secure Web Access with Quick Configuration on page 117
- Configuring Secure Web Access with a Configuration Editor on page 121
- Verifying Secure Web Access on page 122

Secure Web Access Terms

Before configuring secure Web access, become familiar with the terms defined in Table 38.

Table 38: Secure Web Access Terms

Term	Definition
certificate authority (CA)	Third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The CA guarantees the identity of the individual or device that presents the digital certificate.
Hypertext Transfer Protocol (HTTP)	Protocol used to publish and receive information on the Web, such as text and graphics files.

Table 38: Secure Web Access Terms (continued)

Term	Definition
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	Protocol similar to HTTP with an added encryption layer that encrypts and decrypts user page requests and pages that are returned by a Web server. HTTPS is used for secure communication, such as payment transactions.
Privacy-Enhanced Mail (PEM)	Technique for securely exchanging electronic mail over a public medium. PEM is based upon public key infrastructure (PKI) standards like X.509 certificates. SSL certificates are partly based on PEM and end in the suffix .pem.
RSA	Public key cipher that can be used for encrypting messages and making digital signatures. RSA uses a well-known encryption and authentication algorithm that is a part of popular Web browsers.
Secure Sockets Layer (SSL)	Protocol that encrypts security information before transmitting data across a network. SSL requires two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message—and an authentication certificate. Most popular Web browsers support SSL.
SSL certificate	Secure electronic identifier conforming to the X.509 standard, definitively identifying an individual, system, company, or organization. In addition to identification data, the digital certificate contains a serial number, a copy of the certificate holder's public key, the identity and digital signature of the issuing certificate authority (CA), and an expiration date.

Secure Web Access Overview

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

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

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

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

Before You Begin

Before you begin initial configuration, complete the following tasks:

- Establish basic connectivity. See "Establishing Basic Connectivity" on page 93.
- Obtain an SSL certificate from a trusted signing authority. See "Generating SSL Certificates" on page 117.

Generating SSL Certificates

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

To generate an SSL certificate:

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

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

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

2. When prompted, type the appropriate information in the identification form. For example, type US for the country name.

3. Display the contents of the file new.pem.

   cat new.pem

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

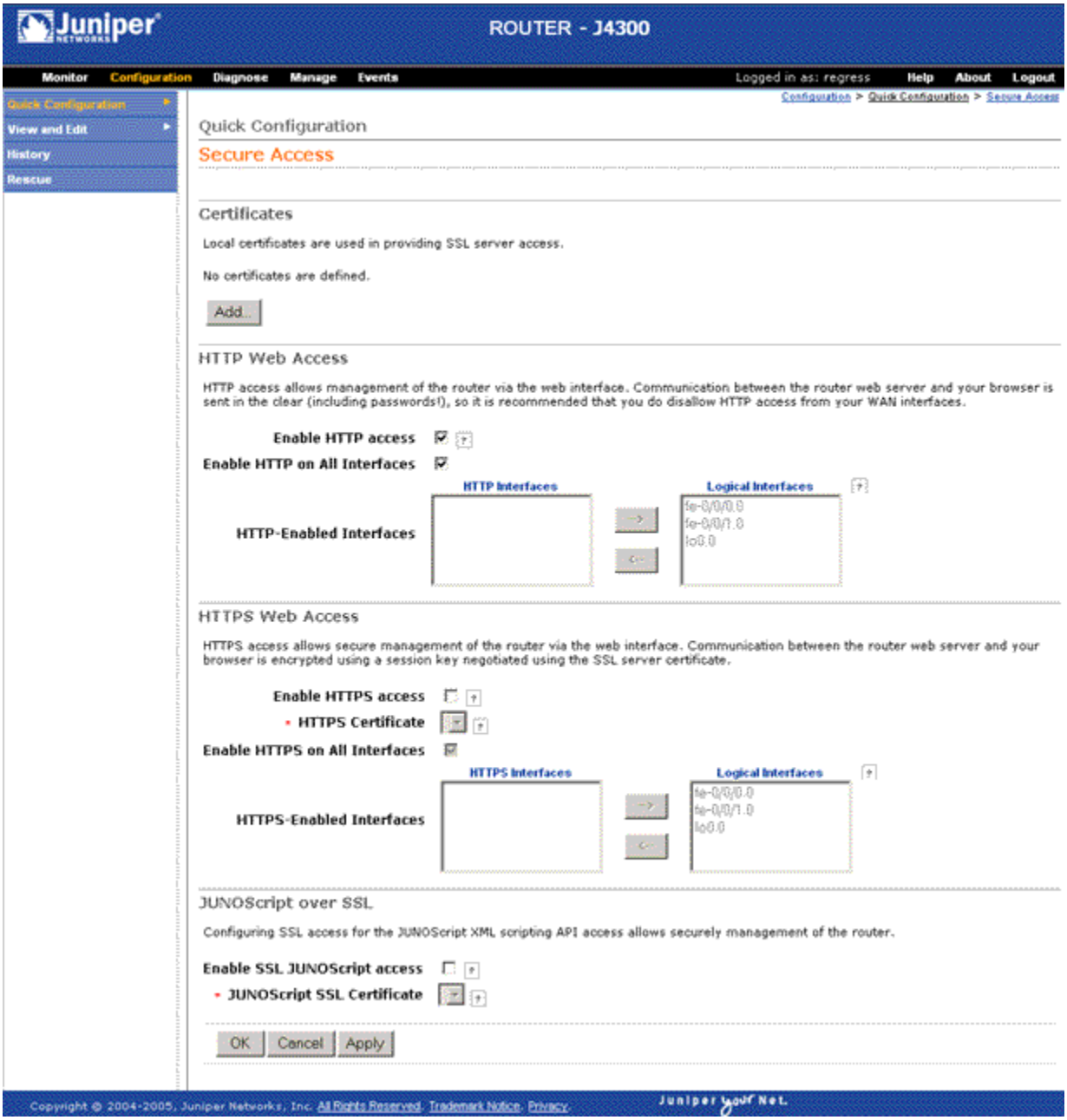
Use can use either J-Web Quick Configuration or a configuration editor to install the SSL certificate and enable HTTPS.

Configuring Secure Web Access with Quick Configuration

Use the Secure Access Quick Configuration page to enable HTTP and HTTPS access on interfaces for managing Services Routers through the Web interface. You can also install SSL certificates and enable JUNOScript over SSL with the Secure Access page.

Figure 37 shows the Secure Access Quick Configuration page.

Figure 37: Quick Configuration Secure Access Page



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

1. Generate an SSL certificate. An SSL certificate is required for enabling HTTPS or SSL JUNOScript access. Skip this step if you are enabling HTTP access. For instructions about generating SSL certificates, see “Generating SSL Certificates” on page 117.

2. In the J-Web user interface, select **Configuration > Quick Configuration > Secure Access**.

3. Enter information into the Secure Access Quick Configuration page, as described in Table 39.

4. Click one of the following buttons:

   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.

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

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

5. To verify that Web access is enabled correctly, connect to the Services Router using one of the following methods:

   - For HTTP access—In your Web browser, type http:// *URL* or http:// *IP address* .

   - For HTTPS access—In your Web browser, type https:// *URL* or https:// *IP address* .

   - For SSL JUNOScript access—A JUNOScript client such as JUNOScope is required. For information about how to log in to JUNOScope, see the *JUNOScope Software User Guide*.

6. To verify the secure Web access configuration, see "Verifying Secure Web Access" on page 122.

Table 39: Secure Access Quick Configuration Summary

Field	Function	Your Action
Certificates		
Certificates	Displays digital certificates required for SSL access to the Services Router. Allows you to add and delete SSL certificates. For information about how to generate an SSL certificate, see "Generating SSL Certificates" on page 117.	To add a certificate: 1. Click **Add**. Opens the Add a Local Certificate page. 2. Type a name in the Certificate Name box—for example, new. 3. Paste the generated certificate and RSA private key in the Certificate box. To delete a certificate, select it and click **Delete**.
Enable HTTP Access		
Enable HTTP Access	Enables HTTP access on interfaces.	To enable HTTP access, select the **Enable HTTP access** check box.
Enable HTTP on All Interfaces	Enables HTTP access on all interfaces at one time.	To enable HTTP access on all interfaces, select the **Enable HTTP on All Interfaces** check box.
HTTP-Enabled Interfaces	Specifies interfaces on which you want to enable HTTP access.	Select and deselect interfaces by clicking the direction arrows: ■ To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. ■ To disable HTTP access on an interface, add the interface to the Logical Interfaces list.
HTTPS Web Access		
Enable HTTPS Access	Enables HTTPS access on interfaces.	To enable HTTPS access, select the **Enable HTTPS access** check box.
HTTPS Certificate	Specifies SSL certificates to be used for encryption. This field is available only after you have created an SSL certificate.	To specify the HTTPS certificate, select a certificate from the HTTPS Certificate list—for example, **new**.
Enable HTTPS on All Interfaces	Enables HTTPS on all interfaces at one time.	To enable HTTPS on all interfaces, select the **Enable HTTPS on All Interfaces** check box.

Table 39: Secure Access Quick Configuration Summary (continued)

Field	Function	Your Action
Certificates		
HTTPS-Enabled Interfaces	Allows you to specify interfaces on which you want to enable HTTPS access.	Select and deselect interfaces by clicking the direction arrows: ■ To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. ■ To disable HTTPS access on an interface, add the interface to the Logical Interfaces list.
JUNOScript over SSL		
Enable SSL JUNOScript access	Enables secured SSL access to the JUNOScript XML scripting API.	To enable SSL access, select the **Enable SSL JUNOScript access** check box.
JUNOScript SSL Certificate	Specifies SSL certificates to be used for encryption. This field is available only after you create at least one SSL certificate.	To enable an SSL certificate, select a certificate from the JUNOScript SSL Certificate list—for example, **new**.

Configuring Secure Web Access with a Configuration Editor

You can manage your Services Router using a secure Web connection by enabling HTTPS.

To enable HTTPS on your Services Router:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 40.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see "Verifying Secure Web Access" on page 122.

Table 40: Configuring a Secure Web Access

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

Table 40: Configuring a Secure Web Access (continued)

Task	J-Web Configuration Editor	CLI Configuration Editor
Import the SSL certificate that you have generated—for example, new. For information about generating SSL certificates, see "Generating SSL Certificates" on page 117.	1. Next to Certificates, click **Configure**. 2. Next to Local, click **Add new entry**. 3. In the Name box, type a name for the certificate to be imported—for example, new. 4. In the Certificate box, paste the generated SSL certificate and private key. 5. Click **OK**.	Enter set certificates local new load-key-file *path* Replace *path* with a path or URL to the file containing an SSL certificate and private key in PEM format—for example, /var/tmp/new.pem
Enable HTTPS access and specify the SSL certificate to be used for authentication. Specify the port on which HTTPS access is to be enabled—for example, TCP port 8443. **NOTE:** You can enable HTTPS access on specified interfaces also. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.	1. On the main Configuration page next to System, click **Configure** or **Edit**. 2. Select the **Services** check box and click **Edit** next to it. 3. Next to Web management, click **Edit**. 4. Select the **Https** check box and click **Edit** next to it. 5. In the Local certificate box, type the name of the certificate—for example, new. 6. In the Port box, type 8443. 7. Click **OK**.	From the [edit system] hierarchy level, enter set services web-management https local-certificate new port 8443

Verifying Secure Web Access

To verify that the Services Router has the secure access settings you configured, perform the following tasks:

- Displaying an SSL Certificate Configuration on page 122
- Displaying a Secure Access Configuration on page 123

Displaying an SSL Certificate Configuration

Purpose Display the SSL certificate configuration.

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

The following sample output displays an SSL certificate generated with instructions in "Generating SSL Certificates" on page 117.

Sample Output

```
[edit]
user@R0# show security
certificates {
   local {
      new {
         "—BEGIN RSA PRIVATE KEY—\nMIICXQIBAAKBgQC/C5UI4frNqbi
         qPwbTiOkJvqoDw2YgYse0Z5zzVJyErgSg954T\nEuHM67Ck8hAOrCnb0YO+SY
         Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXI4viqE7HSsK\n5sQw/UDBIw7/MJ+OpA
         ... KYiFf4CbBBbjIMQJ0HFudW6ISVBsIONkzX+FT\ni95ddka6iIRnArEb4VFCRh+
         e1QBdp1UjziYf7NuzDx4Z\n —END RSA PRIVATE KEY—\n—BEGIN
         CERTIFICATE— \nMIIDjDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQQ ...
         FADCBkTELMAkGA1UEBhMCdXMx\nCzAJBgNVBAgTAmNhMRIwEAYDVQQHEwlzdW5ue
         HB1YnMxDTALBgNVBAMTBGpucHIxJDAiBgkqhkiG\n9w0BCQEWFW5iaGFyZ2F2YUB
         fLUYAnBYmsYWOH\n —END CERTIFICATE—\n"; ## SECRET-DATA
      }
   }
}
```

What It Means

The output shows the intended secure access configuration. For more information about the format of a configuration file, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Displaying a Secure Access Configuration

Purpose

Verify the secure access configuration.

Action

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

The following sample output displays the sample values for secure Web access as configured in Table 40.

Sample Output

```
[edit]
user@R0# show system services
web-management {
   http;
   https {
      port 8443;
      local-certificate new;
   }
}
```

What It Means

The output shows the intended secure access configuration. For more information about the format of a configuration file, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

Chapter 9

Configuring Autoinstallation

If you are setting up many J-series Services Routers, autoinstallation can help automate the configuration process. You can use either the J-Web configuration editor or CLI configuration editor to configure autoinstallation. The J-Web interface does not include Quick Configuration pages for autoinstallation.

This chapter contains the following topics:

- Autoinstallation Terms on page 125
- Autoinstallation Overview on page 126
- Before You Begin on page 127
- Configuring Autoinstallation with a Configuration Editor on page 128
- Verifying Autoinstallation on page 129

Autoinstallation Terms

Before configuring autoinstallation, become familiar with the terms defined in Table 41.

Table 41: Autoinstallation Terms

Term	Definition
autoinstallation	Automatic configuration of a Services Router when it is powered on without a valid configuration file or is configured specifically for autoinstallation. Autoinstallation is useful when deploying multiple Services Routers.
default configuration	Configuration state when a boot file cannot be located during autoinstallation.
host-specific configuration	Configuration state when a specific filename is used during TFTP server requests.

Autoinstallation Overview

Autoinstallation provides automatic configuration when a new Services Router is powered on without a configuration file or for a Services Router configured for autoinstallation. The autoinstallation process begins anytime a Services Router is powered on and a valid configuration file is not found in the nonvolatile RAM (NVRAM). Typically, a configuration file is unavailable when a Services Router is powered on for the first time, or if the configuration file is deleted from the NVRAM. The autoinstallation features is useful deploying multiple Services Router in networks.

This overview contains the following topics:

- Autoinstallation Interfaces on page 126
- Autoinstallation Process on Services Router on page 126
- Automatic Configuration of a New Services Router on page 127

Autoinstallation Interfaces

Autoinstallation can take place through either a management interface or a serial interface on the Services Router. If a LAN interface with High-level Data Link Control (HDLC) encapsulation is found on the Services Router, autoinstallation attempts to obtain an IP address using DHCP requests, bootstrap protocol (BOOTP), or Reverse Address Resolution Protocol (RARP) requests.

If a serial interface with Frame Relay encapsulation is connected, then the Services Router attempts to obtain an IP address using BOOTP requests. On a serial interface without Frame Relay encapsulation, the Services Router uses Serial Line Address Request Protocol (SLARP).

Autoinstallation Process on Services Router

When the Services Router is powered on for the first time, autoinstallation attempts the following on each connected interface simultaneously:

1. The Services Router sends out DHCP, BOOTP, RARP, or SLARP requests to obtain an IP address.
2. If a DHCP server responds, the router obtains the following:
   - An IP address and subnet mask
   - The address of the Trivial File Transfer Protocol (TFTP), Hypertext Transfer Protocol (HTTP), or File Transfer Protocol (FTP) server with the configuration file
   - The IP address of the TFTP server

   Optionally, the hostname of the TFTP server is obtained from the DHCP server. Usually, the TFTP address or name is specified, not both. If the name is

specified, a DNS server must be available to translate the name of the TFTP server into an IP address.

If the TFTP server is not on the same LAN segment as the new Services Router, or if a specific router is required by the network, then the IP address of an intermediary router must be specified. This address is used as the location to receive TFTP requests for autoinstallation.

Automatic Configuration of a New Services Router

After a new Services Router obtains an IP address, autoinstallation attempts to download a configuration file using one of the following methods:

- Host-specific configuration. If the DHCP server specifies the name of the host-specific configuration file (boot file), the specific filename is used in the TFTP server request. The new Services Router makes three unicast TFTP requests for the specified boot file. If these attempts fail, then the router makes three broadcast requests to any available TFTP server looking for the specified boot file.

- Default configuration. If the boot file cannot be located, or the new Services Router does not receive a specified boot filename from the DHCP server, the autoinstallation process then unicasts or broadcasts TFTP requests for a default router configuration file called *network.conf*. The default configuration file, *network.conf*, contains hostname-to-IP address mapping information.

  If there is no entry for the new Services Router, the autoinstallation process sends out a DNS request and attempts to resolve the hostname. If the J-series Services Router can determine its hostname, a TFTP request is sent for the *hostname.conf* file. The variable, *hostname*, is replaced by the hostname of the router. If the new Services Router is unable to map its IP address to a hostname, then TFTP requests are sent for the default configuration file, *router.conf*.

After the configuration file is downloaded from the TFTP server, it is loaded onto the Services Router and committed.

Before You Begin

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

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

- Create a configuration file and place it on a TFTP server on the network. A configuration file can be either of the following:
  - A host-specific file with the name *hostname.conf* where *hostname* is the name of the Services Router.
  - A default configuration file with the minimum configuration necessary to Telnet into the new Services Router for further configuration.
- Physically attach the Services Router to the network using one or more of the following interface types
  - Ethernet
  - Serial with HDLC encapsulation
- If the DHCP response contains only the hostname for the TFTP server, add IP address-to-hostname mapping for the TFTP server to a DNS database file.
- To use an existing router to receive TFTP requests and forward them to the TFTP server, add additional IP addresses of the hosts providing the TFTP service.

If you choose to create a host-specific configuration file, you must also complete the following tasks:

- Configure the DHCP server to provide a configuration filename to the new Services Router. This filename is then used to request a configuration file from a TFTP server. Copy the host-specific configuration to the TFTP server.
- Copy a default configuration file named *network.conf* to the TFTP server. This file contains IP address-to-hostname mappings in the format *ip host ip address hostname* entries. If a host-specific configuration file is not specified by the DHCP server, this file is used to create a hostname for the new Services Router.
- Add the IP address-to-hostname mapping for the new Services Router to a DNS database file.

Configuring Autoinstallation with a Configuration Editor

To configure autoinstallation:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. To configure autoinstallation, perform the configuration tasks described in Table 42.
3. If you are using the J-Web interface, click **Commit** to view a summary of your changes, then click **OK** to commit the configuration. If you are using the CLI, commit the configuration by entering the commit command.

4. To check the configuration, see "Verifying Autoinstallation" on page 129.

Table 42: Configuring Autoinstallation

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the **System** level in the configuration hierarchy.	1. In the J-Web interface, select **Configuration > View and Edit > Edit Configuration**. 2. Next to System, click **Configure** or **Edit**.	From the [edit] hierarchy level, enter edit system
Enable autoinstallation.	Select **Autoinstallation**, and then click **Configure**.	Enter set autoinstallation configuration servers *url*.
Add the configuration servers by specifying the URL address of a server from which to obtain configuration files.	1. Next to Configuration servers, click **Add new entry**. 2. Type the location of the configuration server in the Url box. 3. If a password is required to access the server, type it into the Password box. 4. Click **OK** to return to the Autoinstallation page.	
Configure one or more Ethernet or serial interfaces to perform autoinstallation, and one or two procurement protocols for each interface. The router uses the protocols to send a request for an IP address from the interface. ■ BOOTP—Sends requests over all interfaces. ■ RARP—Sends requests over Ethernet interfaces. ■ SLARP—Sends requests over serial interfaces.	1. Next to Interfaces, click **Add new entry**. 2. Type the name of the interface into the Interface name box. 3. Select one or two types of protocol used by autoinstallation over the interface. You can select **Bootp, Rarp,** or **Slarp**. 4. Click **OK** to return to the Autoinstallation page.	Enter set autoinstallation interfaces *interface-name*, then one of the following protocols: ■ bootp ■ rarp ■ slarp For example, to set two address procurement protocols, enter a command like the following example: set autoinstallation interfaces ge-2/0/0 bootp rarp

Verifying Autoinstallation

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

Verifying Autoinstallation Status

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

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

Sample Output

```
user@host> show system autoinstallation status

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

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

Chapter 10

Installing and Managing J-series Licenses

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

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

This chapter contains the following topics:

- J-series License Overview on page 131
- Before You Begin on page 132
- Managing J-series Licenses with the J-Web Interface on page 133
- Managing J-series Licenses with the CLI on page 136
- Verifying J-series License Management on page 137

J-series License Overview

Each J-series feature license is valid for only a single Services Router. To manage the licenses, you must understand the components of a license key.

This section contains the following topics:

- Software Feature Licenses on page 131
- License Key Components on page 132

Software Feature Licenses

Each feature license is tied to exactly one software feature, and that license is valid for exactly one Services Router. Table 43 lists the Services Router software features that require licenses.

Table 43: J-series Services Router Software Feature Licenses

Licensed Software Feature	License Name
IBM Networking	
Data link switching (DLSw) on all J-series Services Routers	J-series Services Router Software License for Data Link Switching (DLSw) Support
Traffic Analysis	
J-Flow traffic analysis—all configuration statements within the [edit forwarding-options sampling] and [edit forwarding-options accounting] hierarchies.	J-series Services Router Software License for J-Flow Traffic Analysis
BGP Route Reflectors	
Advanced Border Gateway Protocol (BGP) features that enable route reflectors—all configuration statements within the [edit protocols bgp cluster] hierarchy. BGP clusters allow routers to act as route reflectors by enabling the readvertising of BGP routes to internal peers.	J-series Services Router Software License for Advanced Border Router Protocol Support

License Key Components

A license key consists of two parts:

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

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

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

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

Before You Begin

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

- Purchase the licenses you require.
- Establish basic connectivity. See “Establishing Basic Connectivity” on page 93.

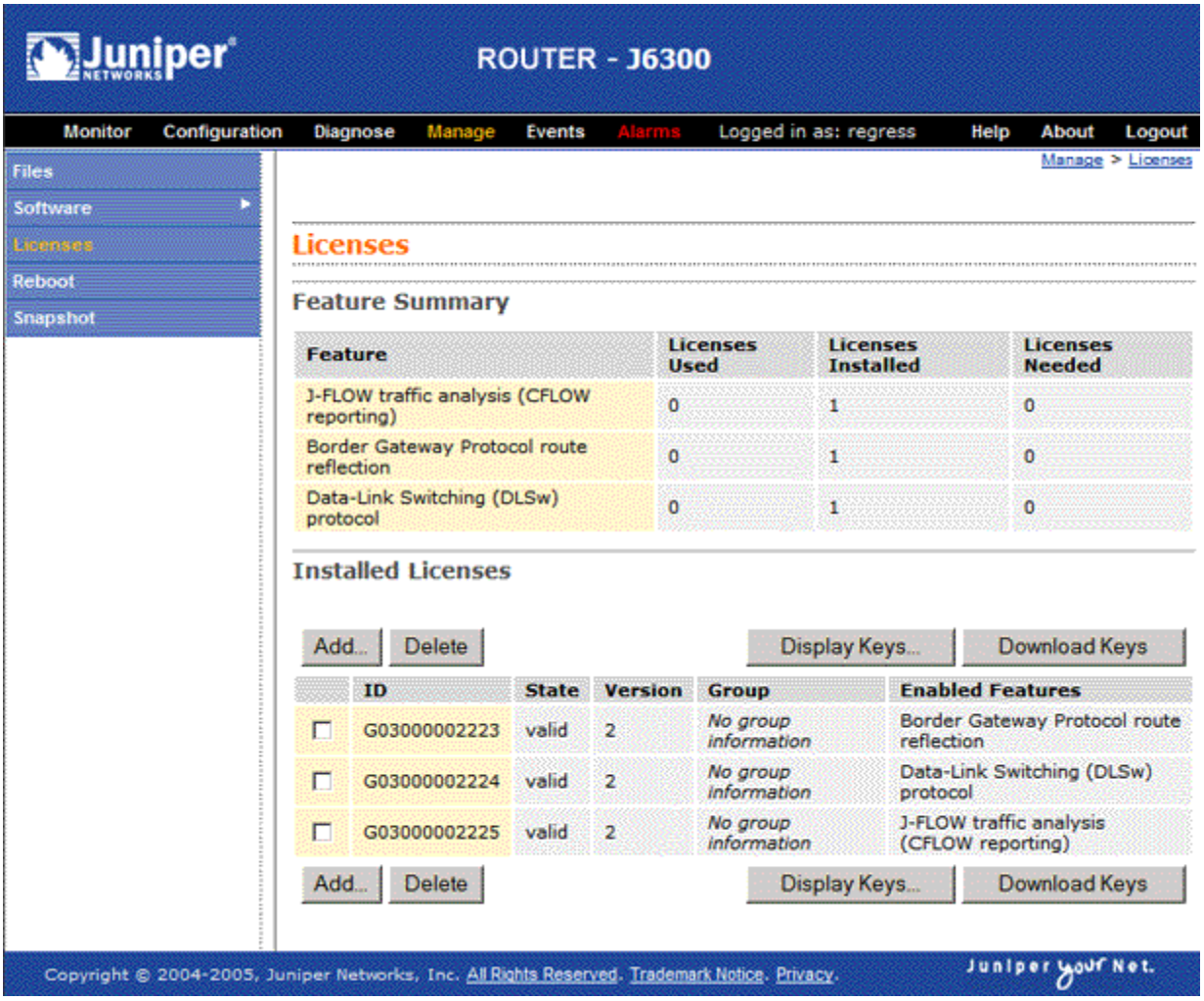
Managing J-series Licenses with the J-Web Interface

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

- Adding New Licenses with the J-Web Interface on page 134
- Deleting Licenses with the J-Web Interface on page 135
- Displaying License Keys with the J-Web Interface on page 135
- Downloading Licenses with the J-Web Interface on page 135

Figure 38 shows the J-Web Licenses page.

Figure 38: Licenses Page



The Licenses page displays a summary of licensed features that are configured on the Services Router and a list of the licenses that are installed on the router. The information on the license management page is summarized in Table 44.

Table 44: Summary of License Management Fields

Field Name	Definition
Feature Summary	
Feature	Name of the licensed feature: ■ J-series licenses listed in Table 43. ■ All features—All-inclusive licenses
Licenses Used	Number of licenses currently being used on the router. Usage is determined by the configuration on the router. If a feature license exists and that feature is configured, the license is considered used.
Licenses Installed	Number of licenses installed on the router for the particular feature.
Licenses Needed	Number of licenses required for legal of use the feature. Usage is determined by the configuration on the router: If a feature is configured and the license for that feature is not installed, a single license is needed.
Installed Licenses	
ID	Unique alphanumeric ID of the license.
State	Valid—The installed license key is valid. Invalid—The installed license key is not valid.
Version	Numeric version number of the license key.
Group	If the license defines a group license, this field displays the group definition. If the license requires a group license, this field displays the required group definition. **NOTE:** Because group licenses are currently unsupported, this field is always blank.
Enabled Features	Name of the feature that is enabled with the particular license.

Adding New Licenses with the J-Web Interface

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

1. In the J-Web interface, select **Manage > Licenses**.
2. Under Installed Licenses, click **Add** to add a new license key.
3. Do *one* of the following, using a blank line to separate multiple license keys:

- In the License File URL box, type the full URL to the destination file containing the license key to be added.
- In the License Key Text box, paste the license key text, in plain-text format, for the license to be added.

4. Click **OK** to add the license key.
5. Go on to "Verifying J-series License Management" on page 137.

Deleting Licenses with the J-Web Interface

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

1. In the J-Web interface, select **Manage > Licenses**.
2. Select the check box of the license or licenses you want to delete.
3. Click **Delete**.
4. Go on to "Verifying J-series License Management" on page 137.

Displaying License Keys with the J-Web Interface

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

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

   A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.
3. Go on to "Verifying J-series License Management" on page 137.

Downloading Licenses with the J-Web Interface

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

1. In the J-Web interface, select **Manage > Licenses**.
2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the router to a single file.

3. Select **Save it to disk** and specify the file to which the license keys are to be written.

4. Go on to "Verifying J-series License Management" on page 137.

Managing J-series Licenses with the CLI

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

- Adding New Licenses with the CLI on page 136
- Deleting a License with the CLI on page 136
- Saving License Keys with the CLI on page 137

Adding New Licenses with the CLI

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

1. Enter operational mode in the CLI.

2. Enter one of the following CLI commands:

   - To add a license key from a file or URL, enter the following command, specifying the filename or the URL where the key is located:

     request system license add *filename* | *url*

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

     request system license add terminal

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

   If the license key you enter is invalid, an error is generated when you press Ctrl-D to exit license entry mode.

4. Go on to "Verifying J-series License Management" on page 137.

Deleting a License with the CLI

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

1. Enter operational mode in the CLI.

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

   request system license delete *license-id*

3. Go on to “Verifying J-series License Management” on page 137.

Saving License Keys with the CLI

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

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

   request system license save *filename* | *url*

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

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

3. Go on to “Verifying J-series License Management” on page 137.

Verifying J-series License Management

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

- Displaying Installed Licenses on page 137
- Displaying License Usage on page 138
- Displaying Installed License Keys on page 139

Displaying Installed Licenses

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

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

Sample Output

```
user@router> show system license

License usage:
                    Licenses     Licenses    Licenses
  Feature name         used    installed      needed
  j-flow                  0            1           0
  bgp-reflection          0            1           0
  dlsw                    0            1           0

Licenses installed:
  License identifier: G03000002223
  State: valid
  License version: 2
  Valid for device: JN001875AB
  Features:
    bgp-reflection   - Border Gateway Protocol route reflection
```

```
License identifier: G03000002224
State: valid
License version: 2
Valid for device: JN001875AB
Features:
  dlsw             - Data-Link Switching (DLSw) protocol

License identifier: G03000002225
State: valid
License version: 2
Valid for device: JN001875AB
Features:
  j-flow           - J-FLOW traffic analysis (CFLOW reporting)
```

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

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

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

Displaying License Usage

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

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

Sample Output

```
user@router> show system license usage

                Licenses     Licenses    Licenses
  Feature name               used       installed    needed
  j-flow                     0            0           1
  bgp-reflection             1            1           0
  dlsw                       1            1           0
```

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

- Each licensed feature is present. Features are listed in ascending alphabetical order by license name. The number of licenses is shown in the third column. Verify that the appropriate number of licenses are installed.

- The number of used licenses matches the number of configured features. If a licensed feature is configured, the feature is considered used. The sample output shows that the DLSw and BGP route reflection features are configured.
- A license is installed on the Services Router for each configured feature. For every feature configured that does not have a license, one license is needed.

  For example, the sample output shows that the user has configured the J-Flow traffic analysis feature but has not purchased the license for it. An additional license is required to be in compliance with license agreements.

Displaying Installed License Keys

Purpose Verify the license keys installed on the Services Router.

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

Sample Output

```
user@router> show system license keys

G03000002223 aeaqea qkjjhd ambrha 3tkqkc ayareb zicik6
             nv6jck btlxao 2trfyq 65cdou r5tbbb xdarpg
             qq53lu qcx4vm ydakcs t3yyh2 v5mq

G03000002224 aeaqea qkjjhd ambrha 3tkqkc ayargb zicik6
             nv6jck btlxao 2trfyq 65cdou r5tbof l4uon5
             7rokz7 wgdocl r4q32p 2wu4zf zrxa

G03000002225 aeaqea qkjjhd ambrha 3tkqkc ayarab zicik6
             nv6jck btlxao 2trfyq 65cdou r5tbiu jr6ui2
             lmqgqj ouzq5a aiokdn 4tr4u2 wmcq
```

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

Part 3

Maintaining Services Router Hardware

- Replacing and Troubleshooting Hardware Components on page 143
- Contacting Customer Support and Returning Hardware on page 175

Chapter 11

Replacing and Troubleshooting Hardware Components

Because many of the Services Router's hardware components are field-replaceable units (FRUs), you can remove and replace them yourself. When you need to replace a router component, contact your customer support or sales representative to order the field-replaceable unit (FRU) that contains the component. For instructions, see "Contacting Customer Support and Returning Hardware" on page 175.

This chapter contains the following topics:

- Replacing Hardware Components on page 143
- Troubleshooting Hardware Components on page 171

Replacing Hardware Components

This section contains the following topics:

- Tools and Parts Required on page 144
- Replacing the Console Port Cable on page 144
- Replacing a PIM on page 144
- Replacing PIM Cables on page 147
- Replacing the Compact Flash Disk on page 149
- Removing and Installing the USB Storage Device on page 153
- Removing and Installing DRAM Modules on page 155
- Replacing Power System Components on page 158
- Removing and Installing a Crypto Accelerator Module on page 167
- Replacing an Air Filter on page 170

Tools and Parts Required

To replace hardware components, you need the tools and parts listed in Table 45.

Table 45: Tools and Parts Required

Tool or Part	Components
Electrostatic bag or antistatic mat	All
Electrostatic discharge (ESD) grounding wrist strap	All
Flat-blade screwdriver, approximately 1/4 in. (6 mm)	PIM
Phillips (+) screwdriver, number 2	■ Compact flash ■ Crypto Accelerator Module ■ DRAM modules ■ Power system components

Replacing the Console Port Cable

The RJ-45 port labeled CONSOLE on the Services Router's front panel allows you to connect the router to an external management device, such as a laptop or a terminal server. For cable specifications, see "Network Cable Specifications and Connector Pinouts" on page 185.

To replace the console port cable:

1. Locate an appropriate replacement cable and connector.
2. Plug the Ethernet connector at either end of the cable into the console port on the front panel (see Figure 36).
3. Plug the connector at the other end of the cable into the external management device. If you are connecting to a DB-9 serial port, use the provided RJ-45 to DB-9 serial port adapter.

Replacing a PIM

To remove or install field-replaceable Physical Interface Modules (PIMs) in a Services Router, you must first power off the router. This section contains the following topics:

- Removing a PIM on page 145
- Installing a PIM on page 146

Removing a PIM

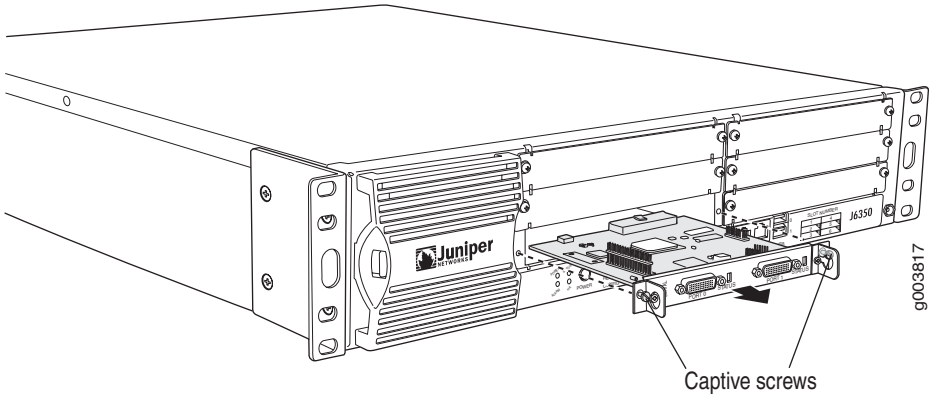
The PIMs are installed in the front of the Services Router. A PIM weighs less than 1 lb (0.5 kg).

CAUTION: Do not hot-swap PIMs. Failure to power off the router before removing or installing a PIM might result in damage to the hardware.

To remove a PIM (see Figure 39):

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the PIM.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the Services Router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
3. Press and release the power button to power off the router. Verify that the POWER LED blinks and then turns off.
4. Label the cables connected to the PIM so that you can later reconnect each cable to the correct PIM.
5. Disconnect the cables from the PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
   - Secure each cable so that it is not supporting its own weight as it hangs to the floor.
   - Place excess cable out of the way in a neatly coiled loop.
   - Use fasteners to maintain the shape of cable loops.
7. Loosen the captive screws on each side of the PIM faceplate.
8. Grasp the handles on each side of the PIM faceplate, and slide the PIM out of the router. Place it in the electrostatic bag or on the antistatic mat.
9. If you are not reinstalling a PIM into the emptied slot, install a blank PIM panel over the slot to maintain proper airflow.

Figure 39: Removing a PIM



Installing a PIM

CAUTION: Do not hot-swap PIMs. Failure to power off the router before removing or installing a PIM might result in damage to the hardware.

To install a PIM (see Figure 40):

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the Services Router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.
2. Press and release the power button to power off the router. Verify that the POWER LED blinks and then turns off.
3. Align the notches in the connector at the rear of the PIM with the notches in the PIM slot in the Services Router, and slide the PIM in until it lodges firmly in the router.

CAUTION: Slide the PIM straight into the slot to avoid damaging the components on the PIM.

4. Tighten the captive screws on each side of the PIM faceplate.
5. Insert the appropriate cables into the cable connectors on the PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:

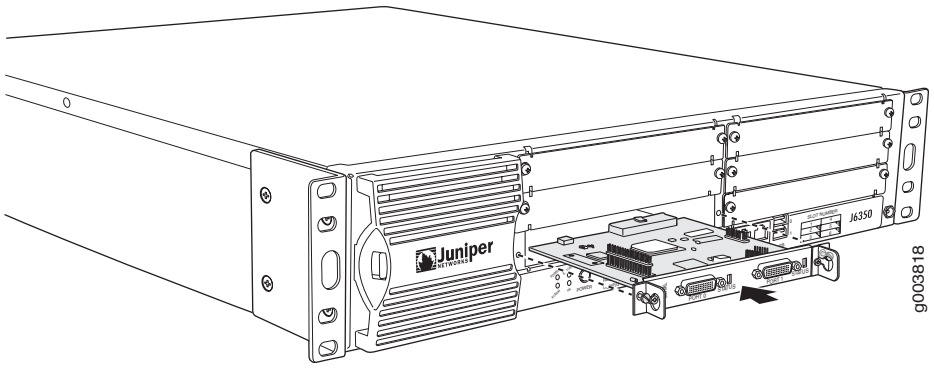
- Secure each cable so that it is not supporting its own weight as it hangs to the floor.
- Place excess cable out of the way in a neatly coiled loop.
- Use fasteners to maintain the shape of cable loops.

7. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.
8. Verify that the PIM LEDs light steadily green to confirm that the PIM and its ports are online and operational. For more information about PIM LEDs, see "Field-Replaceable PIMs" on page 29.

   You can also verify correct PIM functioning by issuing the show chassis fpc pic-status command described in the *JUNOS System Basics and Services Command Reference*.

NOTE: In the show chassis fpc pic-status command, the PIM slot number is reported as an FPC number and the PIM number (always 0) is reported as a PIC number.

Figure 40: Installing a PIM



Replacing PIM Cables

Removing and installing PIM cables does not affect Services Router function, except that a PIM does not receive or transmit data while its cable is disconnected. To replace a PIM cable, perform the following procedures:

- Removing a PIM Cable on page 148
- Installing a PIM Cable on page 148

Removing a PIM Cable

To remove a PIM cable:

1. If you are removing all cables connected to the PIM, issue the following CLI command to take the PIM offline:

   ```
   user@host> request chassis pic fpc-slot pim-slot pic-slot 0 offline
   ```

   For example, to take the PIM in slot 4 offline, enter the following command:

   ```
   user@host> request chassis pic fpc-slot 4 pic-slot 0 offline
   ```

   For more information about the command, see the *JUNOS System Basics and Services Command Reference*.

2. Unplug the cable from the cable connector port.

3. Detach the cable from the destination port.

Installing a PIM Cable

To install a PIM cable:

1. Have ready a length of the type of cable used by the PIM. For cable specifications, see "Network Cable Specifications and Connector Pinouts" on page 185.

2. Insert the cable connector into the cable connector port on the PIM faceplate.

3. Arrange the cable as necessary to prevent it from dislodging or developing stress points:

   - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
   - Place excess cable out of the way in a neatly coiled loop.
   - Use fasteners to maintain the shape of cable loops.

4. Insert the other end of the cable into the destination port.

5. Repeat the previous steps for any additional cables.

6. If the PIM is offline (its status LED is steadily red), issue the following CLI command to bring the PIM online:

   ```
   user@host> request chassis pic fpc-slot pim-slot pic-slot 0 online
   ```

   For example, to bring the PIM in slot 4 online, enter the following command:

   ```
   user@host> request chassis pic fpc-slot 4 pic-slot 0 online
   ```

For more information about the command, see the *JUNOS System Basics and Services Command Reference*.

7. Verify that the PIM status LED shines steadily green to confirm that the PIM is online.

   You can also verify correct PIM functioning by issuing the show chassis fpc pic-status command described in the *JUNOS System Basics and Services Command Reference*.

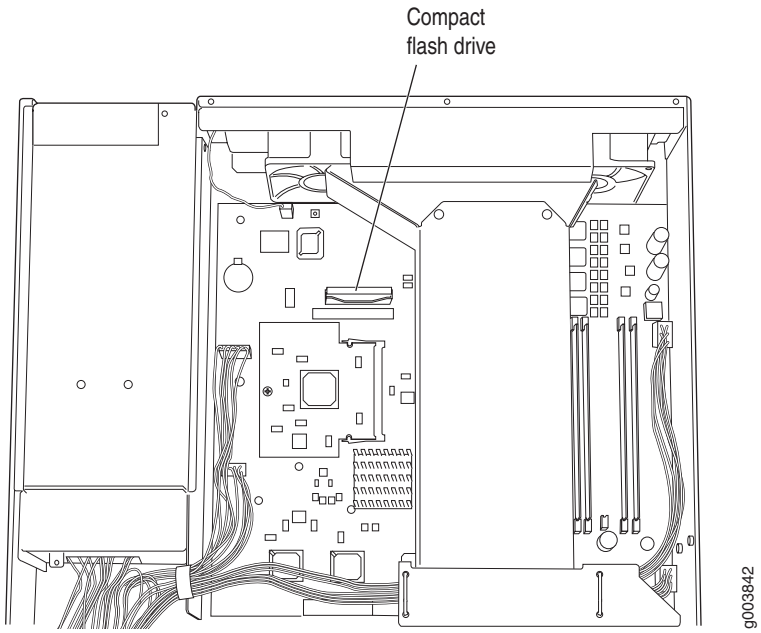
NOTE: In the show chassis fpc pic-status command, the PIM slot number is reported as an FPC number and the PIM number (always 0) is reported as a PIC number.

Replacing the Compact Flash Disk

The primary compact flash drive is installed in a slot on the Routing Engine (see Figure 41).

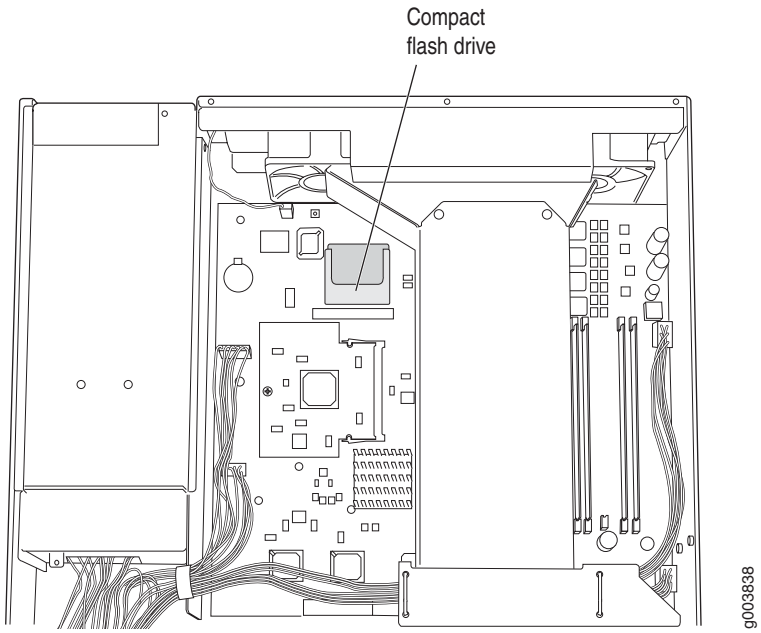
NOTE: Use only compact flash disks purchased from Juniper Networks for your J-series platform and model.

Figure 41: Location of Compact Flash Disk



On some Services Routers, the compact flash is in a horizontal position, while on others it is in a vertical position. Figure 42 shows the alternative horizontal orientation of the compact flash.

Figure 42: Alternative Horizontal Orientation of Compact Flash Disk



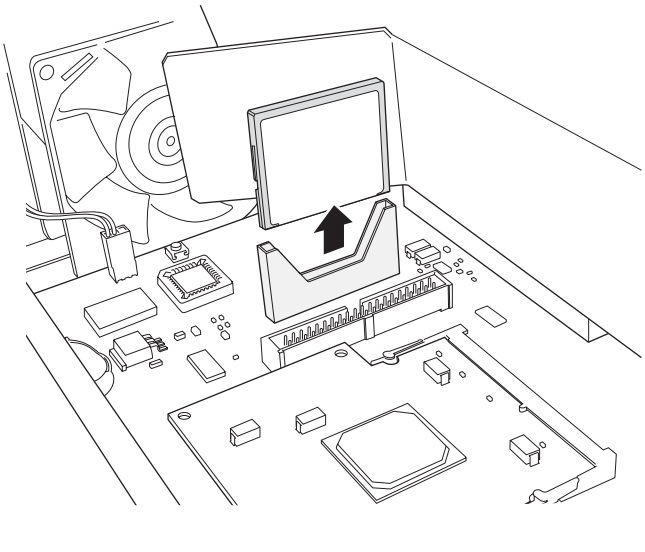
To replace the compact flash disk:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.
3. Press and release the power button to power off the router. Wait for the POWER LED to turn off.
4. Remove the power cord or cable from the power source receptacle.
5. Remove the screws from the sides and top of the chassis that secure the cover to the chassis.
6. Slide the cover off the chassis.

WARNING: If the fans are still rotating, wait until they stop before proceeding with the next step, especially if your compact flash is in the horizontal position (flat against the bottom of the chassis).

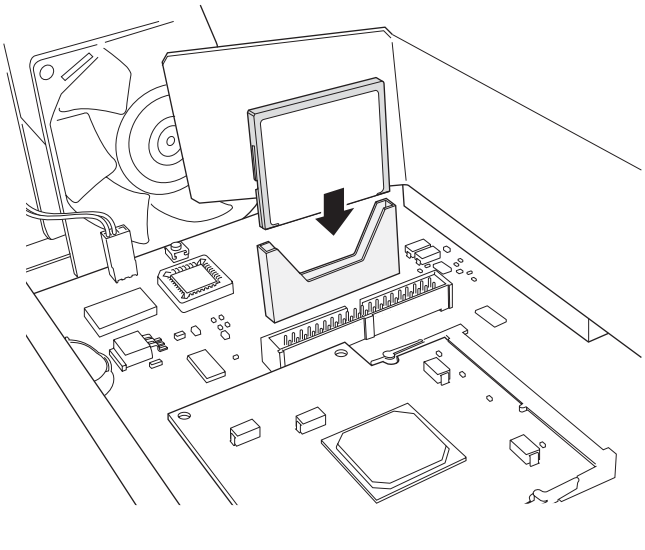
7. Slide the compact flash disk out of its slot, as shown in Figure 43.

Figure 43: Removing the Compact Flash Disk



8. Place the compact flash disk on the antistatic mat or in the electrostatic bag.
9. Slide the new compact flash disk into the slot and press down, as shown in Figure 44.

Figure 44: Inserting the Compact Flash Disk



NOTE: On some Services Routers the compact flash is in a horizontal position. If the compact flash connection is horizontal, lay the compact flash behind the slot and slide it forward until it clicks into place.

10. Slide the cover onto the chassis.
11. Replace and tighten the screws on the sides and top of the chassis that secure the cover to the chassis.
12. Replace the power cord or cable.
13. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

Removing and Installing the USB Storage Device

USB storage devices are optional components on J-series Services Routers. If installed, a USB storage device provides secondary storage for the router. It can accommodate software images, configuration files, and microcode. If the primary compact flash disk fails on startup, and the removable compact flash disk is not installed or fails, the router boots from the USB storage device.

For information about configuring the USB storage device, see the *J-series Services Router Administration Guide*.

NOTE: For a list of supported USB storage devices, see the *J-series Services Router Release Notes* at http://www.juniper.net.

To remove and install a USB storage device, perform the following procedures:

- Removing the USB Storage Device on page 154
- Installing the USB Storage Device on page 155

Removing the USB Storage Device

NOTE: Depending on your configuration, the Services Router might not have a USB storage device. If no USB storage device is installed, proceed directly to the next section, "Installing the USB Storage Device" on page 155.

The USB storage device is installed into the USB port on the front panel of the Services Router. To remove the USB storage device:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
3. Verify that the router did not boot from the USB storage device by issuing the show system storage command from the CLI. For example:

   ```
   user@host> show system storage
   Filesystem        512-blocks       Used      Avail Capacity Mounted on
   /dev/ad0s1a           218254     175546      40526     81%  /
   ...
   ```

   The boot device is mounted on /. The primary compact flash disk is located at ad0. The USB storage device is located at da0. This example shows that the router booted from the primary compact flash disk.
4. If the show system storage output indicates that the router booted from the USB storage device, press and release the power button to power off the router. Wait for the POWER LED to turn off before you remove the USB storage device.
5. Gently grasp the USB storage device and slide it out of the USB port.
6. Place the USB storage device on the antistatic mat or in the electrostatic bag.

Installing the USB Storage Device

To install the USB storage device:

NOTE: For a list of supported USB storage devices, see the *J-series Services Router Release Notes* at http://www.juniper.net.

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
2. Orient the USB storage device with the USB port on the front panel of the router.
3. Insert the USB storage device into the USB port. If the USB storage device does not easily slide into the port, it might not be oriented correctly. Turn the USB storage device upside-down and try again.
4. To configure the USB storage device with the request system snapshot command, see the *J-series Services Router Administration Guide*.

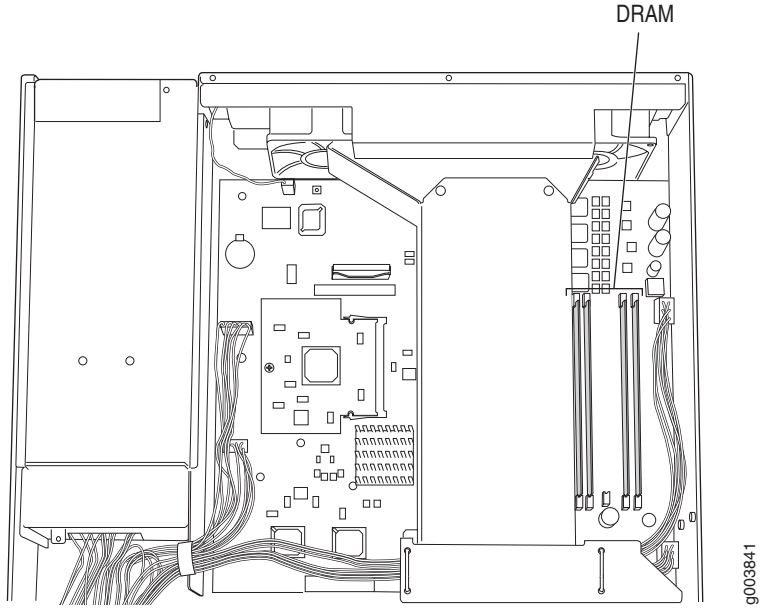
Removing and Installing DRAM Modules

The DRAM installed on the Routing Engine provides storage for the routing and forwarding tables and for other Routing Engine processes. The design of the Routing Engine allows you to modify the DRAM configuration by adding DRAM modules to the Routing Engine board, or removing DRAM modules from the board.

The DRAM modules are located on the top of the Routing Engine, as shown in Figure 45.

NOTE: Use only DRAM modules purchased through Juniper Networks specifically for your model. Also, DRAM modules are not always transferable across J-series platforms. You can use the same DRAM module in both the J4350 and J6350 Services Routers. However, do not use a DRAM from another J-series platform in a J4350 or J6350 router.

Figure 45: J4350 and J6350 DRAM Location



To modify the DRAM configuration, use the following procedures:

- Removing a DRAM Module on page 156
- Installing a DRAM Module on page 157

Removing a DRAM Module

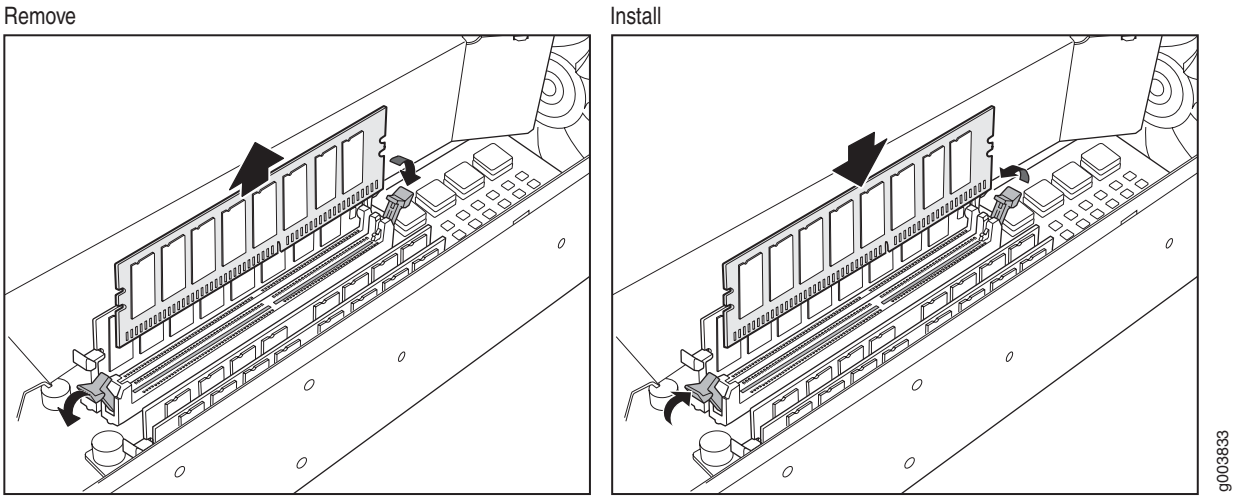
NOTE: Depending on your configuration, the Services Router might have an empty DRAM socket. If you are adding a DRAM module to the DRAM configuration, proceed directly to "Installing a DRAM Module" on page 157.

To remove a DRAM module:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see the Getting Started Guide for your router.

3. Press and release the power button to power off the router. Wait for the POWER LED to turn off.
4. Unplug the power cord or cable from the power source receptacle.
5. Remove the screws from the sides and top of the chassis that secure the cover to the chassis.
6. Slide the cover off the chassis.
7. To release the DRAM module, press the plastic ejectors on both sides of the module (see Figure 46).
8. Grasp the DRAM module, being careful not to touch any electrical components on the module, and firmly pull it out of the slot on the Routing Engine.
9. Place the DRAM module on the antistatic mat or in the electrostatic bag.

Figure 46: Adding or Replacing a DRAM Module



Installing a DRAM Module

The J4350 and J6350 Services Routers support 256-MB and 512-MB DRAM modules. Use only DRAM modules purchased from Juniper Networks specifically for your model.

NOTE: If you are installing a second DRAM module, install it in a socket in one of the opposite pair of sockets from the first DRAM module. This configuration might provide better performance than installing two DRAM modules in adjacent sockets.

To install a DRAM module onto the Routing Engine:

1. Take the following steps if you have not already done so:

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

   b. Press and release the power button to power off the router. Wait for the POWER LED to turn off.

   c. Unplug the power cord or cable from the power source receptacle.

   d. Remove the screws from the sides and top of the chassis that secure the cover to the chassis.

   e. Slide the cover off the chassis.

2. Remove the DRAM module from its electrostatic bag.

3. To open the empty DRAM socket, press the plastic ejectors on both sides (see Figure 46).

4. Grasp the DRAM module by the edges, being careful not to touch any electrical components.

5. Pressing firmly on both ends, push the module into the socket until the ejectors click into the closed position (see Figure 46).

6. Slide the cover onto the chassis.

7. Replace and tighten the screws on the sides and top of the chassis that secure the cover to the chassis.

8. Replace the power cord or cable.

9. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

10. To view the DRAM configuration and verify that it was installed correctly, issue the show chassis routing-engine command, described in the *JUNOS System Basics and Services Command Reference*. This command shows the total memory installed.

Replacing Power System Components

The power cords on all Services Routers are replaceable.

You can replace AC or DC power supplies in any Services Router. You can also add a second power supply to the J6350 Services Router that is of the same type as the first (either AC or DC).

The power supplies are located at the right rear of the chassis (see Figure 3 and Figure 5). Each power supply provides power to all components in the router. The

power supplies are fully redundant. If one power supply fails or is removed, the remaining power supply instantly assumes the entire electrical load. One power supply can provide full power for as long as the router is operational.

Each J6350 power supply is hot-insertable and hot-removable.

CAUTION: Do not leave a power supply slot empty for more than a short time while the Services Router is operational. The power supply or a blank power supply panel must remain in the chassis for proper airflow.

To replace power system components, use the following procedures:

- Replacing an AC Power Supply Cord on page 159
- Removing an AC Power Supply from a J6350 Router on page 160
- Installing an AC Power Supply in a J6350 Router on page 161
- Replacing a DC Power Supply Cable on page 162
- Removing a DC Power Supply from a J6350 Router on page 163
- Installing a DC Power Supply in a J6350 Router on page 165

Replacing an AC Power Supply Cord

To replace the AC power cord for a redundant power supply:

1. Locate a replacement power cord with the type of plug appropriate for your geographical location (see "AC Power, Connection, and Power Cord Specifications" on page 76).
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
3. Press and release the power button to power off the router. Wait for the POWER LED to turn off.

NOTE: If the power supply is a redundant power supply in a J6350 Services Router, you can leave the router powered on and power flowing in the alternate power supply.

4. Unplug the power cord from the power source receptacle.
5. Unplug the power cord from the appliance inlet on the power supply faceplate.

6. Insert the appliance coupler end of the replacement power cord into the appliance inlet on the power supply faceplate.

7. Insert the power cord plug into an AC power source receptacle.

NOTE: Each power supply must be connected to a dedicated AC power feed. For information about connecting to AC power sources, see "Connecting Power" on page 86.

8. Verify that the power cord does not block access to Services Router components or drape where people might trip on it.

9. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

Removing an AC Power Supply from a J6350 Router

The power supplies are located at the right rear of the chassis. A power supply weighs 2.4 lb (1.1 kg).

To remove an AC power supply from a J6350 Services Router (see Figure 47):

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.

2. Press and release the power button to power off the Services Router. Wait for the POWER LED to turn off.

NOTE: If the power supply is a redundant power supply in a J6350 Service Router, you can leave the router powered on and power flowing in the alternate power supply.

3. Unplug the power cord from the power source receptacle.

4. Unplug the power cord from the appliance inlet on the power supply faceplate.

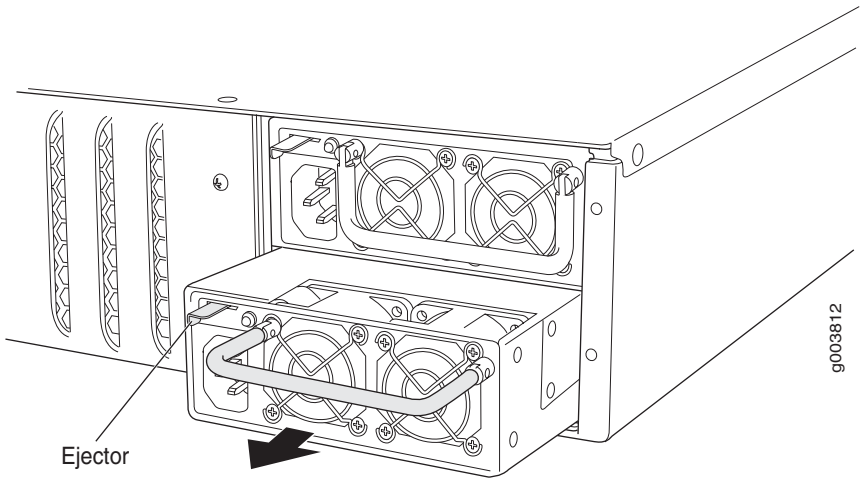
5. Slide the ejector tab on the power supply faceplate to the right and hold it in place to unlock the power supply.

6. Grasp the handle on the power supply faceplate, and pull firmly to start removing the power supply. Slide it halfway out of the chassis (see Figure 47).

7. Place one hand underneath the power supply to support it and slide it completely out of the chassis.

8. If you are not reinstalling a power supply into the emptied slot, install a blank power supply panel over the slot.

Figure 47: Removing an AC Power Supply



Installing an AC Power Supply in a J6350 Router

To install an AC power supply in a J6350 Services Router (see Figure 48):

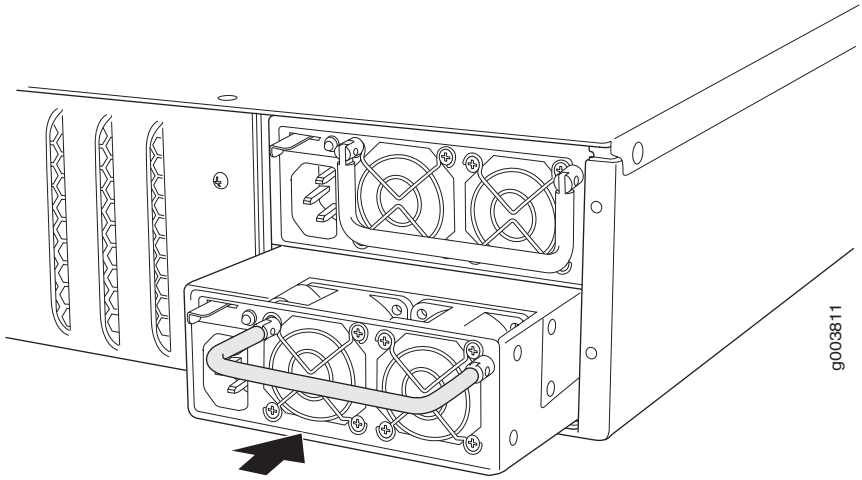
1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.
2. Using both hands, slide the power supply into the chassis until you feel resistance.
3. Firmly push the power supply into the chassis until it comes to a stop. Make sure that the power supply faceplate is flush with any adjacent power supply faceplate.
4. Insert the appliance coupler end of a power cord into the appliance inlet on the power supply faceplate.
5. Insert the power cord plug into an AC power source receptacle.

NOTE: Each power supply must be connected to a dedicated AC power feed. For information about connecting to AC power sources, see “Connecting Power” on page 86.

6. Verify that the power cord does not block access to router components or drape where people might trip on it.

7. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

Figure 48: Installing an AC Power Supply



Replacing a DC Power Supply Cable

To replace a power cable for a DC power supply:

1. Locate a replacement power cable and a lug that meet the specifications defined in “Chassis Grounding” on page 86 and “DC Power, Connection, and Power Cable Specifications” on page 77.

CAUTION: A licensed electrician must attach a cable lug to the power cable that you supply. A cable with an incorrectly attached lug can damage the router (for example, by causing a short circuit).

---

2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.

3. Press and release the power button to power off the Services Router. Wait for the POWER LED to turn off.

4. Ensure that the voltage across the DC power source cable leads is 0 V and that the cable leads cannot become active during installation.

CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity.

5. Remove the power cable from the DC power source.
6. Use a Phillips screwdriver to remove the clear plastic cover protecting the terminal block.
7. Within the terminal block, remove the screw that fastens the power cable lug to the terminal block.
8. Carefully move the power cable out of the way.
9. Using the removed screw, secure the replacement power cable to the appropriate terminal. Tighten the screw until snug. Do not overtighten.

   The screw contains a captive washer used to secure the power cable lug to the terminal block.

NOTE: Each power supply must be connected to a dedicated DC power feed. For information about connecting to DC power sources, see "Connecting Power" on page 86.

10. Dress the power cable appropriately.
11. Replace the clear plastic cover over the terminal block.
12. Verify that the power cable does not block access to router components or drape where people might trip on it.
13. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

Removing a DC Power Supply from a J6350 Router

The power supplies are located at the right rear of the chassis. A power supply weighs 2.4 lb (1.1 kg).

To remove a DC power supply from a J6350 Services Router (see Figure 49):

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if

the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.

2. Press and release the power button to power off the Services Router. Wait for the POWER LED to turn off.

3. Ensure that the voltage across the DC power source cable leads is 0 V and that the cable leads cannot become active during installation.

CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity.

---

4. Remove the power cables from the DC power source.

5. Use a Phillips screwdriver to remove the clear plastic cover protecting the terminal block.

6. Within the terminal block, remove the screws that fasten the power cable lugs to the terminal block.

7. Carefully move the power cables out of the way.

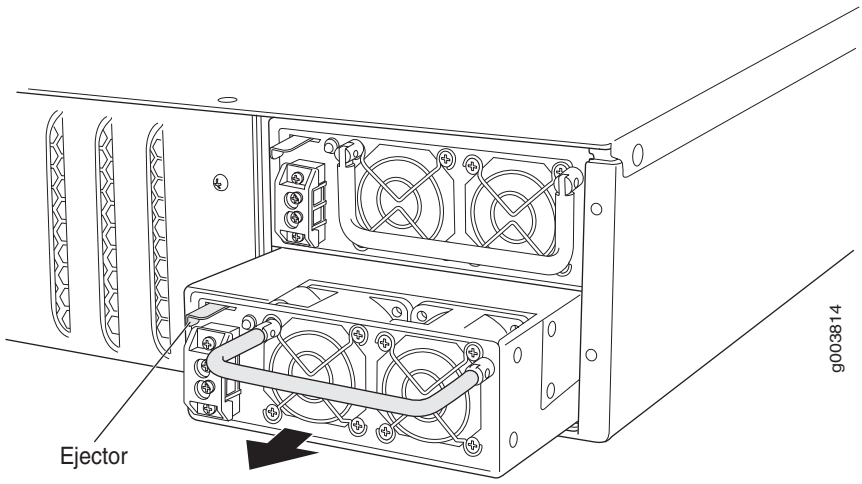
8. Slide the ejector tab on the power supply faceplate to the right, and hold it in place to unlock the power supply.

9. Grasp the handle on the power supply faceplate, and pull firmly to start removing the power supply. Slide it halfway out of the chassis (see Figure 49).

10. Place one hand underneath the power supply to support it, and slide it completely out of the chassis.

11. If you are not reinstalling a power supply into the emptied slot, install a blank power supply panel over the slot.

Figure 49: Removing a DC Power Supply



Installing a DC Power Supply in a J6350 Router

Each power supply in a DC-powered router must be connected to earth ground. A ground terminal is provided on each DC power supply for this purpose.

To install a DC power supply in a J6350 Services Router (see Figure 50):

1. Ensure that the voltage across the DC power source cable leads is 0 V and that the cable leads cannot become active during installation.

CAUTION: There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply. You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity.

---

2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.

3. Using both hands, slide the power supply into the chassis until you feel resistance.

4. Firmly push the power supply into the chassis until it comes to a stop. Make sure that the power supply faceplate is flush with any adjacent power supply faceplate.

5. Use a Phillips screwdriver to remove the clear plastic cover protecting the terminal block.

6. Within the terminal block, remove the two center screws next to the labels –48 VDC and RTN.

   Each screw contains a captive washer to secure a power cable lug to the terminal block.

7. Using one of the removed screws, secure the positive (+) DC source power cable lug to the RTN terminal. Tighten the screw until snug. Do not overtighten. Apply between 8 lb-in. (0.9 Nm) and 9 lb-in. (1.02 Nm) of torque to the screw.

8. Using the other removed screw, secure the negative (–) DC source power cable lug to the –48 VDC terminal. Tighten the screw until snug. Do not overtighten. Apply between 8 lb-in. (0.9 Nm) and 9 lb-in. (1.02 Nm) of torque to the screw.

NOTE: Each power supply must be connected to a dedicated DC power feed. For information about connecting to DC power sources, see "Connecting Power" on page 86.

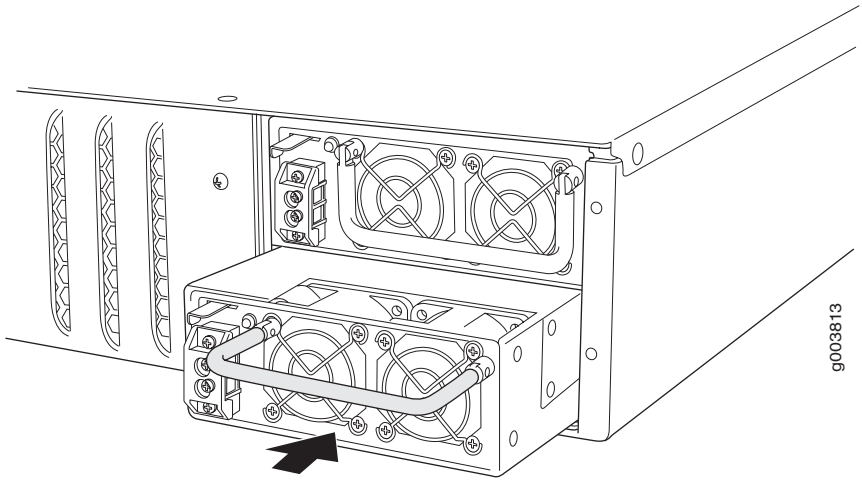
9. Dress the power cables appropriately.

10. Replace the clear plastic cover over the terminal block.

11. Verify that the power cord does not block access to router components or drape where people might trip on it.

12. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

Figure 50: Installing a DC Power Supply

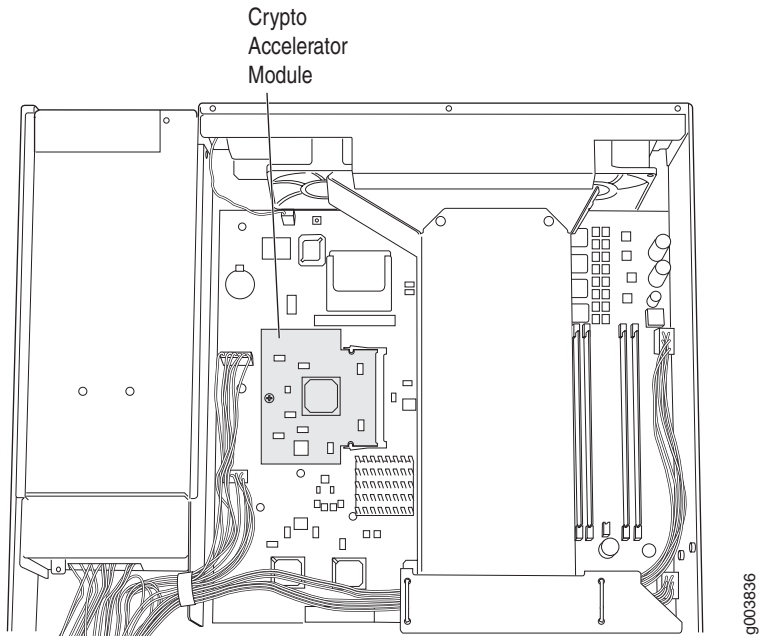


Removing and Installing a Crypto Accelerator Module

The Crypto Accelerator Module is a processor card that enhances performance of cryptographic algorithms used in IP security (IPSec) services. The Crypto Module is a standard feature on J6350 Services Routers and an optional feature on J4350 Services Routers.

Figure 51 shows the location of the Crypto Accelerator Module.

Figure 51: Crypto Accelerator Module Location



To modify a Crypto Accelerator Module configuration, use the following procedures:

- Removing the Crypto Accelerator Module on page 167
- Installing a Crypto Accelerator Module on page 169

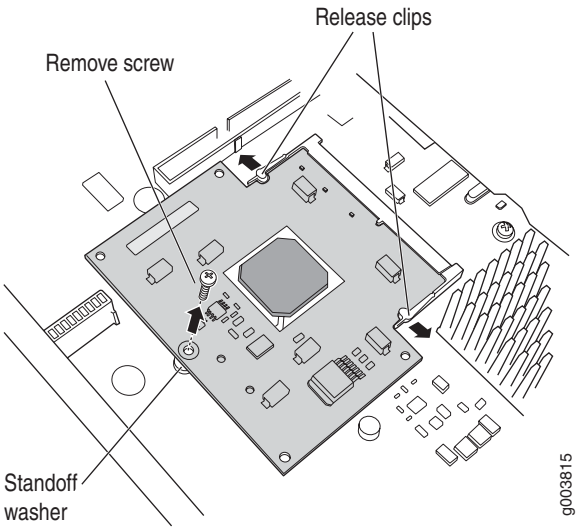
Removing the Crypto Accelerator Module

NOTE: If you are installing a Crypto Accelerator Module into a J4350 Services Router for the first time, proceed directly to "Installing a Crypto Accelerator Module" on page 169.

To remove the Crypto Accelerator Module:

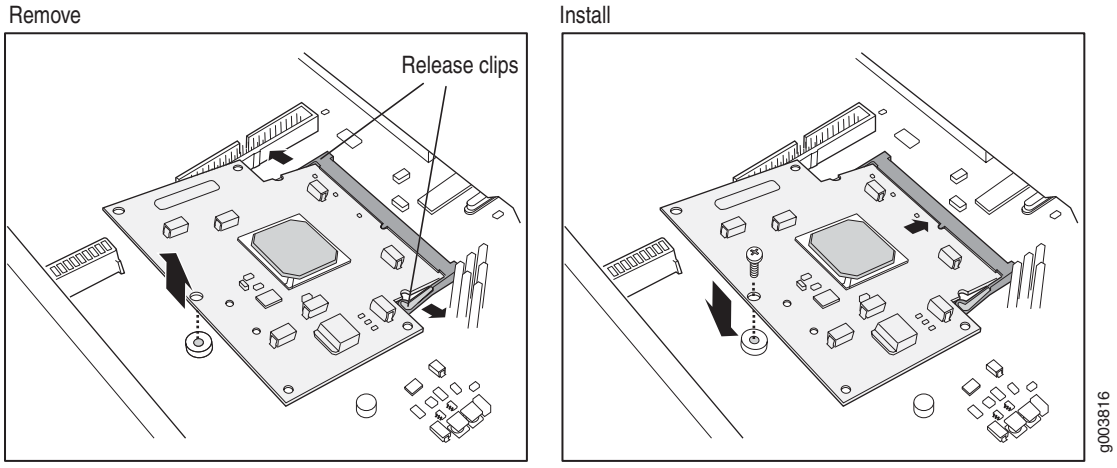
1. Place an electrostatic bag or antistatic mat on a flat stable surface to receive the Crypto Module.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 205.
3. Press and release the power button to power off the Services Router. Wait for the POWER LED to turn off.
4. Unplug the power cord or cable from the power source receptacle.
5. Remove the screws from the sides and the top of the chassis, and slide the cover off the chassis.
6. Locate the Crypto Module on the system board (see Figure 51).
7. Remove the screw, as shown in Figure 52.

Figure 52: Removing the Crypto Module Screw



8. Pull the white release clips on either side of the Crypto Module out to either side, as shown in Figure 53, to tilt the Crypto Module upward.

Figure 53: Removing and Installing a Crypto Accelerator Module



9. Slide the Crypto Module out of its socket.
10. Remove the standoff washer that was under the Crypto Module.
11. Place the Crypto Module on the antistatic mat or in the electrostatic bag.

Installing a Crypto Accelerator Module

To install a Crypto Accelerator Module:

1. Take the following steps if you have not already done so:
   a. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
   b. Press and release the power button to power off the Services Router. Wait for the POWER LED to turn off.
   c. Unplug the power cord or cable from the power source receptacle.
   d. Remove the screws from the sides and the top of the chassis, and slide the cover off the chassis.
2. Locate the Crypto Module socket on the system board (see Figure 51). The socket is tipped up at an angle when empty.
3. If a screw and standoff washer are already in place (see Figure 52), remove them.
4. Remove the Crypto Module from its electrostatic bag and insert it into the socket.

5. Push the Crypto Module down flat against the main board until the release clips click into place, as shown in Figure 53.

6. Insert the standoff washer under the Crypto Module.

7. Insert the screw and tighten it until snug. Do not overtighten.

8. Slide the cover onto the router, and replace and tighten the cover screws.

9. Replace the power cord or cable.

10. Press and release the power button to power on the router. Verify that the POWER LED lights steadily after you press the power button.

11. Verify that the Crypto Module is correctly installed by issuing the show chassis hardware command, as shown in the following example:

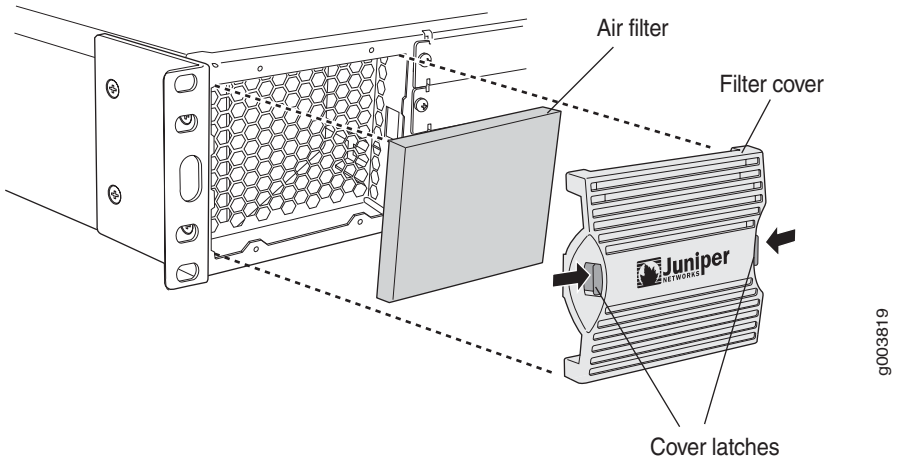
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN1086A34ADA      J4350
Midplane         REV 00   710-014594
System IO        REV 00   710-012315                     JX350 System IO
Routing Engine   REV 00   710-012149                     RE-J4350-2540
Crypto Module                                           Crypto acceleration
FPC 0                                                   FPC
  PIC 0                                                 4x GE Base PIC
```

If Crypto Module appears in the output, the Crypto Accelerator Module is installed correctly.

Replacing an Air Filter

The front panel of J4350 and J6350 Services Routers contains an air intake grid with a protective cover and a filter, as shown in Figure 54.

Figure 54: Attaching Air Filter and Filter Cover



We recommend changing the filter every 6 months. However, the optimal filter replacement interval can vary depending on the environment where the router is located. If temperature alarms appear, inspect the air filter.

To replace the air filter:

1. Remove the filter cover by squeezing the plastic tabs on either side of the filter cover.
2. Pull the filter cover away from the chassis.
3. Remove the old filter.
4. Place the new filter in the opening.
5. Replace the filter cover by pressing it until it clicks into place.

Troubleshooting Hardware Components

This section provides an overview of the resources you can use to troubleshoot hardware problems on the Services Router:

- Chassis Alarm Conditions on page 171
- Contacting the Juniper Networks Technical Assistance Center on page 173

Chassis Alarm Conditions

When the Routing Engine detects an alarm condition, it lights the ALARM LED on the front panel. When the condition is corrected, the light turns off.

To view a more detailed description of the alarm cause, issue the show chassis alarms CLI command:

```
user@host> show chassis alarms
```

Table 46 describes alarms that can occur for a chassis component such as the Routing Engine or a Physical Interface Module (PIM).

Table 46: Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Corrective Action	Alarm Severity
Alternative boot media	The Services Router boots from an alternative boot device.	Typically, the router boots from the primary compact flash disk. If you configured your router to boot from an alternative boot device, ignore this alarm condition. If you did not configure the router to boot from an alternative boot device, contact JTAC. (See "Requesting Support" on page xx.)	Yellow (minor)
PIM	A PIM has failed. When a PIM fails, it attempts to reboot. If the Routing Engine detects that a PIM is rebooting too often, it shuts down the PIM.	Replace the failed PIM. (See "Replacing a PIM" on page 144.)	Red (major)

Table 46: Chassis Alarm Conditions and Corrective Actions (continued)

Component	Alarm Conditions	Corrective Action	Alarm Severity
Routing Engine	An error occurred during the process of reading or writing compact flash.	Reformat the compact flash and install a bootable image. (See the *J-series Services Router Administration Guide*.) If this remedy fails, you must replace the failed Routing Engine. To contact JTAC, see "Requesting Support" on page xx.	Yellow (minor)
	Routing Engine temperature is too warm.	■ Check the room temperature. (See "Router Environmental Tolerances" on page 73.) ■ Check the air flow. (See "General Site Guidelines" on page 71.) ■ Check the fans. (See "Cooling System" on page 22.) If you must replace a fan or the Routing Engine, contact JTAC. (See "Requesting Support" on page xx.) ■ Check the air filter and replace it if it appears clogged. (See "Replacing an Air Filter" on page 170)	Yellow (minor)
	Routing Engine temperature is too hot.		Red (major)
	Routing Engine fan has failed.	Replace the failed fan. To contact JTAC, see "Requesting Support" on page xx.	Red (major)

Contacting the Juniper Networks Technical Assistance Center

If you need assistance while troubleshooting a Services Router, open a support case using the Case Manager link at http://www.juniper.net/support/, or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

Chapter 12

Contacting Customer Support and Returning Hardware

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

- Locating Component Serial Numbers on page 175
- Contacting Customer Support on page 178
- Return Procedure on page 178
- Packing a Router or Component for Shipment on page 179

Locating Component Serial Numbers

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

```
    user@host> show chassis hardware
 Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                               015810200500      J6350
Midplane         REV 00   710-012339
System IO        REV 00   710-012315                     JX350 System IO
Routing Engine   REV 00   710-012151      RE-J6350-3400
HW crypto                                                Crypto accelerator
FPC 0                                                    FPC
  PIC 0                                                  4x GE Base
PIC
```

NOTE: In the show chassis hardware command, the PIM slot number is reported as an FPC number and the PIM number (always 0) is reported as the PIC number.

Most components also have a serial number ID label (see Figure 56) attached to the component body.

J4350 and J6350 Services Routers have two serial number ID labels, one on the back of the chassis, as shown in Figure 55, and one on the bottom front corner, as shown in Figure 56.

Figure 55: Location of Serial Number ID Label on Back of Chassis

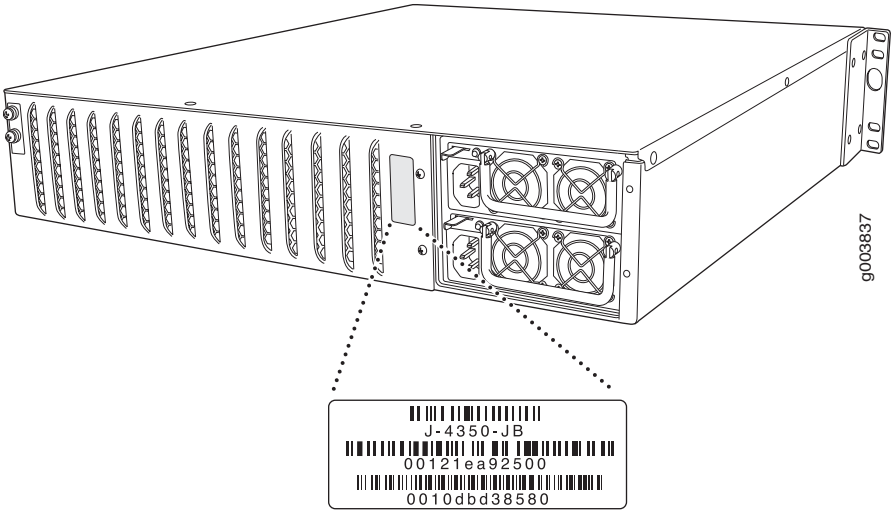
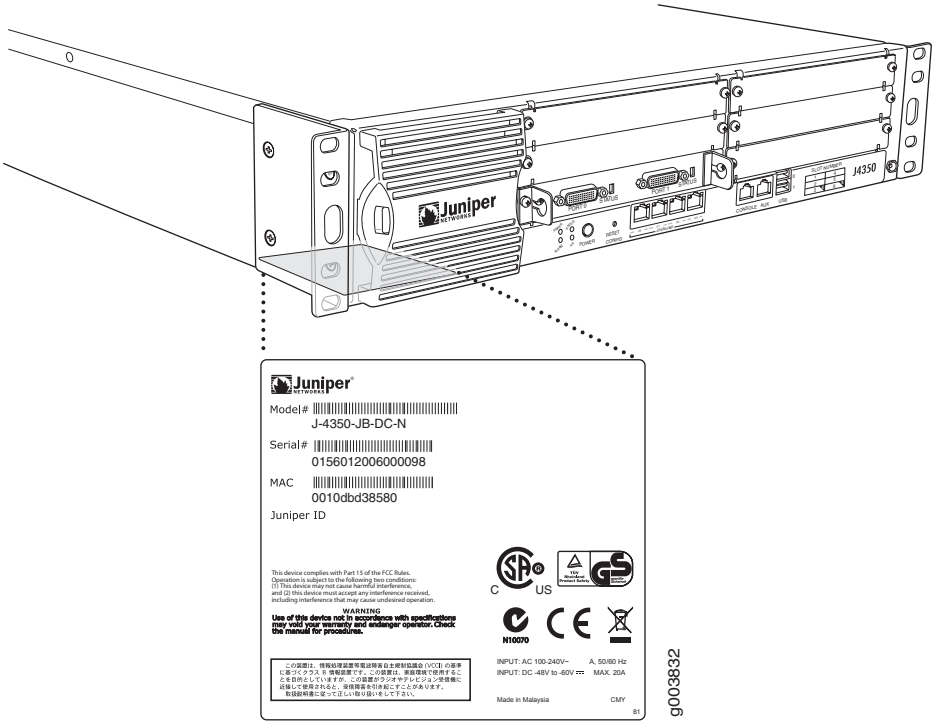


Figure 56: Location of Serial Number ID Label on Bottom of Chassis



Serial ID label

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

- PIM Serial Number Label on page 177
- J6350 Power Supply Serial Number Labels on page 177

PIM Serial Number Label

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

J6350 Power Supply Serial Number Labels

The power supplies installed in the J6350 Services Router are field-replaceable. Each power supply has a unique serial number. The serial number label is located on the top of the power supply.

Contacting Customer Support

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

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

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

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

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

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

Information You Might Need to Supply to JTAC

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

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

Return Procedure

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

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

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

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

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

1. Determine the part number and serial number of the component. For instructions, see "Locating Component Serial Numbers" on page 175.
2. Obtain a Return Materials Authorization (RMA) number from the Juniper Networks Technical Assistance Center (JTAC). You can send e-mail or telephone as described above.
3. Provide the following information in your e-mail message or during the telephone call:
   - Part number and serial number of component
   - Your name, organization name, telephone number, and fax number
   - Description of the failure
4. The support representative validates your request and issues an RMA number for return of the component.
5. Pack the router or component for shipment, as described in "Packing a Router or Component for Shipment" on page 179.

Packing a Router or Component for Shipment

This section contains the following topics:

- Tools and Parts Required on page 179
- Packing the Services Router for Shipment on page 180
- Packing Components for Shipment on page 181

Tools and Parts Required

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

- Blank panels to cover empty slots
- Electrostatic bag or antistatic mat, for each component
- Electrostatic discharge (ESD) grounding wrist strap

- Flat-blade screwdriver, approximately 1/4 in. (6 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Packing the Services Router for Shipment

To pack the router for shipment, follow this procedure:

1. Retrieve the shipping carton and packing materials in which the router was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 205.
3. On the console or other management device connected to the master Routing Engine, enter CLI operational mode and issue the following command to shut down the router software.

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

   Wait until a message appears on the console confirming that the operating system has halted. For more information about the command, see the *J-series Services Router Administration Guide*.
4. Shut down power to the router by pressing the power button on the front panel of the router.
5. Disconnect power from the router. For instructions, see "Replacing an AC Power Supply Cord" on page 159.
6. Remove the cables that connect to all external devices. For instructions, see "Removing a PIM Cable" on page 148.
7. Remove all field-replaceable units (FRUs) from the router.
8. If the router is installed on a wall or rack, have one person support the weight of the router, while another person unscrews and removes the mounting screws.
9. Place the router in the shipping carton.
10. Cover the router with an ESD bag, and place the packing foam on top of and around the router.
11. Replace the accessory box on top of the packing foam.
12. Securely tape the box closed.
13. Write the RMA number on the exterior of the box to ensure proper tracking.

Packing Components for Shipment

To pack and ship individual components, follow these guidelines:

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

CAUTION: Do not stack any of the router components.

Part 4

J-series Requirements and Specifications

- Network Cable Specifications and Connector Pinouts on page 185
- Safety and Regulatory Compliance Information on page 201

Chapter 13

Network Cable Specifications and Connector Pinouts

The network interfaces supported on the router accept different kinds of network cable.

- Serial PIM Cable Specifications on page 185
- RJ-45 Connector Pinout for Fast Ethernet Ports on page 194
- RJ-45 Connector Pinout for Gigabit Ethernet Ports on page 195
- Console Port Pinouts on page 195
- E1 and T1 RJ-48 Cable Pinouts on page 196
- E3 and T3 BNC Connector Pinout on page 198
- ADSL and G.SHDSL RJ-11 Connector Pinout on page 199
- ISDN RJ-45 Connector Pinout on page 199

Serial PIM Cable Specifications

The 2-port serial PIM uses the cables and connectors summarized in Table 47. Pinouts are detailed in Table 48 through Table 57.

Table 47: 2-Port Serial PIM Cables and Connectors

Name	Connector	Connector Hardware	End-to-End Conductors	Pinouts
RS-232 DTE	DB-25 male	4-40 threaded jackscrews	13	Table 48
RS-232 DCE	DB-25 female	4-40 threaded jacknuts	13	Table 49
RS-422/449 (EIA-449) DTE	DC-37 (DB-37) male	4-40 threaded jackscrews	25	Table 50
RS-422/449 (EIA-449) DCE	DC-37 (DB-37) female	4-40 threaded jacknuts	25	Table 51

Table 47: 2-Port Serial PIM Cables and Connectors (continued)

Name	Connector	Connector Hardware	End-to-End Conductors	Pinouts
EIA-530A DTE	DB-25 male	4-40 threaded jackscrews	23	Table 52
EIA-530A DCE	DB-25 female	4-40 threaded jacknuts	22	Table 53
V.35 DTE	M/34 male	Standard (Normally included with M/34 connector shell)	18	Table 54
V.35 DCE	M/34 female	Standard (Normally included with M/34 connector shell)	18	Table 55
X.21 DTE	DB-15 male	M3 threaded jackscrews	13	Table 56
X.21 DCE	DB-15 female	M3 threaded jacknuts	13	Table 57

RS-232 DTE Cable Pinout

Table 48: RS-232 DTE Cable Pinout

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
15	1	–	Frame Ground
60	2	–	Transmit Data
1	3	–	Receive Data
48	4	–	Request to Send
37	5	–	Clear to Send
9	6	–	Data Set Ready
57	7	–	Signal Ground
13	8	–	Data Carrier Detect
56	15	–	Transmit Clock
5	17	–	Receive Clock
41	18	–	Local Loopback
33	20	–	Data Terminal Ready
52	24	–	Terminal Clock

Table 48: RS-232 DTE Cable Pinout (continued)

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
22 to 21	–	–	–
18 to 17	–	–	–

RS-232 DCE Cable Pinout

Table 49: RS-232 DCE Cable Pinout

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
15	1	–	Frame Ground
1	2	–	Transmit Data
60	3	–	Receive Data
37	4	–	Request to Send
48	5	–	Clear to Send
33	6	–	Data Set Ready
57	7	–	Signal Ground
13	8	–	Data Carrier Detect
56	15	–	Transmit Clock
52	17	–	Receive Clock
45	18	–	Local Loopback
9	20	–	Data Terminal Ready
5	24	–	Terminal Clock
22 to 21	–	–	–

RS-422/449 (EIA-449) DTE Cable Pinout

Table 50: RS-422/449 (EIA-449) DTE Cable Pinout

LFH-60 Pin	DC-37 (DB-37) Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
60	4	59	Send Data (A)
56	5	55	Send Timing (A)
1	6	2	Receive Data (A)
48	7	47	Request to Send (A)
5	8	6	Receive Timing (A)

Table 50: RS-422/449 (EIA-449) DTE Cable Pinout (continued)

LFH-60 Pin	DC-37 (DB-37) Pin	LFH-60 Pairing	Description
37	9	38	Clear to Send (A)
41	10	–	Local Loopback
9	11	10	Data Mode (A)
33	12	34	Terminal Ready (A)
13	13	14	Receive Ready (A)
52	17	51	Terminal Timing (A)
36	19	–	Signal Ground
4	20	–	Receive Common
59	22	60	Send Data (B)
55	23	56	Send Timing (B)
2	24	1	Receive Data (B)
47	25	48	Request to Send (B)
6	26	5	Receive Timing (B)
38	27	37	Clear to Send (B)
10	29	9	Data Mode (B)
34	30	33	Terminal Ready (B)
14	31	13	Receiver Ready (B)
51	35	52	Terminal Timing (B)
57	37	–	Send Common
26 to 25	–	–	–
18 to 17	–	–	–

RS-422/449 (EIA-449) DCE Cable Pinout

Table 51: RS-422/449 (EIA-449) DCE Cable Pinout

LFH-60 Pin	DC-37 (DB-37) Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
1	4	2	Send Data (A)
56	5	55	Send Timing (A)
60	6	59	Receive Data (A)
37	7	38	Request to Send (A)
52	8	51	Receive Timing (A)
48	9	47	Clear to Send (A)
45	10	–	Local Loopback

Table 51: RS-422/449 (EIA-449) DCE Cable Pinout (continued)

LFH-60 Pin	DC-37 (DB-37) Pin	LFH-60 Pairing	Description
33	11	34	Data Mode (A)
9	12	10	Terminal Ready (A)
13	13	14	Receive Ready (A)
5	17	6	Terminal Timing (A)
36	19	–	Signal Ground
4	20	–	Receive Common
2	22	1	Send Data (B)
55	23	56	Send Timing (B)
59	24	60	Receive Data (B)
38	25	37	Request to Send (B)
51	26	52	Receive Timing (B)
47	27	48	Clear to Send (B)
34	29	33	Data Mode (B)
10	30	9	Terminal Ready (B)
14	31	13	Receiver Ready (B)
6	35	5	Terminal Timing (B)
57	37	–	Send Common
26 to 25	–	–	–

EIA-530A DTE Cable Pinout

Table 52: EIA-530A DTE Cable Pinout

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
60	2	59	Transmit Data (A)
1	3	2	Receive Data (A)
48	4	47	Request to Send (A)
37	5	38	Clear to Send (A)
9	6	–	Data Set Ready (A)
57	7	–	Signal Ground
13	8	14	Received Line Signal Detector (A)
6	9	5	Receive Clock (B)

Table 52: EIA-530A DTE Cable Pinout (continued)

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
14	10	13	Received Line Signal Detector (B)
51	11	52	Terminal Timing (B)
55	12	56	Transmit Clock (B)
38	13	37	Clear to Send (B)
59	14	60	Transmit Data (B)
56	15	55	Transmit Clock (A)
2	16	1	Receive Data (B)
5	17	6	Receive Clock (A)
41	18	–	Local Loopback
47	19	48	Request to Send (B)
33	20	–	Data Terminal Ready (A)
4	23	–	Signal Ground
52	24	51	Terminal Timing (A)
26 to 25	–	–	–
30 to 29	–	–	–
18 to 17	–	–	–

EIA-530A DCE Cable Pinout

Table 53: EIA-530A DCE Cable Pinout

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
1	2	2	Transmit Data (A)
60	3	59	Receive Data (A)
37	4	38	Request to Send (A)
48	5	47	Clear to Send (A)
33	6	–	Data Set Ready (A)
57	7	–	Signal Ground
13	8	14	Received Line Signal Detector (A)
51	9	52	Receive Clock (B)
14	10	13	Received Line Signal Detector (B)
6	11	5	Terminal Timing (B)

Table 53: EIA-530A DCE Cable Pinout (continued)

LFH-60 Pin	DB-25 Pin	LFH-60 Pairing	Description
55	12	56	Transmit Clock (B)
47	13	48	Clear to Send (B)
2	14	1	Transmit Data (B)
56	15	55	Transmit Clock (A)
59	16	60	Receive Data (B)
52	17	51	Receive Clock (A)
45	18	–	Local Loopback
38	19	37	Request to Send (B)
9	20	–	Data Terminal Ready (A)
4	23	–	Signal Ground
5	24	6	Terminal Timing (A)
26 to 25	–	–	–
30 to 29	–	–	–

V.35 DTE Cable Pinout

Table 54: V.35 DTE Cable Pinout

LFH-60 Pin	M/34 Pin	LFH-60 Pairing	Description
15	A	–	Frame Ground
57	B	–	Signal Ground
48	C	–	Request to Send
37	D	–	Clear to Send
9	E	–	Data Set Ready
13	F	–	Received Line Signal Detector
33	H	–	Data Terminal Ready
41	K	–	Test Mode
60	P	59	Transmit Data (A)
1	R	2	Receive Data (A)
59	S	60	Transmit Data (B)
2	T	1	Receive Data (B)
52	U	51	Terminal Timing (A)
5	V	6	Receive Timing (A)
51	W	52	Terminal Timing (B)
6	X	5	Receive Timing (B)

Table 54: V.35 DTE Cable Pinout (continued)

LFH-60 Pin	M/34 Pin	LFH-60 Pairing	Description
56	Y	55	Transmit Timing (A)
55	AA	56	Transmit Timing (B)
22 to 21	–	–	–
26 to 25	–	–	–
18 to 17	–	–	–

V.35 DCE Cable Pinout

Table 55: V.35 DCE Cable Pinout

LFH-60 Pin	M/34 Pin	LFH-60 Pairing	Description
15	A	–	Frame Ground
57	B	–	Signal Ground
37	C	–	Request to Send
48	D	–	Clear to Send
33	E	–	Data Set Ready
13	F	–	Received Line Signal Detector
9	H	–	Data Terminal Ready
45	K	–	Test Mode
1	P	2	Transmit Data (A)
60	R	59	Receive Data (A)
2	S	1	Transmit Data (B)
59	T	60	Receive Data (B)
5	U	6	Terminal Timing (A)
52	V	51	Receive Timing (A)
6	W	5	Terminal Timing (B)
51	X	52	Receive Timing (B)
56	Y	55	Transmit Timing (A)
55	AA	56	Transmit Timing (B)

Table 55: V.35 DCE Cable Pinout (continued)

LFH-60 Pin	M/34 Pin	LFH-60 Pairing	Description
22 to 21	–	–	–
26 to 25	–	–	–

X.21 DTE Cable Pinout

Table 56: X.21 DTE Cable Pinout

LFH-60 Pin	DB-15 Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
60	2	59	Transmit Data (A)
48	3	47	Control (A)
1	4	2	Receive (A)
37	5	38	Indicate (A)
5	6	6	Signal Element Timing (A)
57	8	–	Signal Ground
59	9	60	Transmit Data (B)
47	10	48	Control (B)
2	11	1	Receive (B)
38	12	37	Indicate (B)
6	13	5	Signal Element Timing (B)
30 to 29	–	–	–
18 to 17	–	–	–

X.21 DCE Cable Pinout

Table 57: X.21 DCE Cable Pinout

LFH-60 Pin	DB-15 Pin	LFH-60 Pairing	Description
15	1	–	Shield Ground
1	2	2	Transmit Data (A)
37	3	38	Control (A)
60	4	59	Receive (A)
48	5	47	Indicate (A)
52	6	51	Signal Element Timing (A)

Table 57: X.21 DCE Cable Pinout (continued)

LFH-60 Pin	DB-15 Pin	LFH-60 Pairing	Description
57	8	–	Signal Ground
2	9	1	Transmit Data (B)
38	10	37	Control (B)
59	11	60	Receive (B)
47	12	48	Indicate (B)
51	13	52	Signal Element Timing (B)
30 to 29	–	–	–

RJ-45 Connector Pinout for Fast Ethernet Ports

Table 58 describes the RJ-45 connector pinout information.

NOTE: Either a straight-through or cross-over cable can be used to connect to the interface.

Table 58: Fast Ethernet RJ-45 Connector Pinout

Pin	Signal
1	TX +
2	TX-
3	RX +
4	Termination network
5	Termination network
6	RX-

Table 58: Fast Ethernet RJ-45 Connector Pinout (continued)

Pin	Signal
7	Termination network
8	Termination network

RJ-45 Connector Pinout for Gigabit Ethernet Ports

Table 59: Gigabit Ethernet RJ-45 Connector Pinout

Pin	Signal
1	MDI0 +
2	MDI0-
3	MDI1 +
4	MDI2 +
5	MDI2-
6	MDI1-
7	MDI3 +
8	MDI3-

Console Port Pinouts

The console port on a J-series Services Router has an RJ-45 connector. Table 60 provides RJ-45 console connector pinout information. An RJ-45 cable is supplied with the router.

To connect the console port to an external management device, you need an RJ-45 to DB-9 serial port adapter, which is also supplied with the router.

Table 60: RJ-45 Console Connector Pinout

Pin	Signal	Description
1	RTS Output	Request to Send
2	DTR Output	Data Terminal Ready
3	TxD Output	Transmit Data
4	GND	Chassis Ground
5	GND	Chassis Ground
6	RxD Input	Receive Data

Table 60: RJ-45 Console Connector Pinout (continued)

Pin	Signal	Description
7	DSR Input	Data Set Ready
8	CTS Input	Clear to Send

Table 61 describes the DB-9 connector pinouts.

Table 61: DB-9 Console Connector Pinout

Pin	Signal	Direction	Description
1	DCD	<–	Carrier Detect
2	RxD	<–	Receive Data
3	TxD	–>	Transmit Data
4	DTR	–>	Data Terminal Ready
5	Ground	—	Signal Ground
6	DSR	<–	Data Set Ready
7	RTS	–>	Request To Send
8	CTS	<–	Clear To Send
9	RING	<–	Ring Indicator

E1 and T1 RJ-48 Cable Pinouts

The E1 and T1 PIMs use an RJ-48 cable, which is not supplied with the PIM.

CAUTION: To maintain agency approvals, use only a properly constructed, shielded cable.

Table 62 through Table 65 describe the RJ-48 connector pinouts.

Table 62: RJ-48 Connector to RJ-48 Connector (Straight) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data Numbering Form)	RJ-48 Pin (Data Numbering Form)	Signal
1	1	RX, Ring, –
2	2	RX, Tip, +
4	4	TX, Ring, –
5	5	TX, Tip, +

Table 62: RJ-48 Connector to RJ-48 Connector (Straight) Pinout (continued)

RJ-48 Pin (on T1/E1 PIM) (Data Numbering Form)	RJ-48 Pin (Data Numbering Form)	Signal
3	3	Shield/Return/Ground
6	6	Shield/Return/Ground
7	No connect	No connect
8	No connect	No connect

Table 63: RJ-48 Connector to RJ-48 Connector (Crossover) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data numbering form)	RJ-48 Pin (Data numbering form)	Signal
1	4	RX/Ring/– <––> TX/Ring/–
2	5	RX/Tip/+ <––> TX/Tip/+
4	1	TX/Ring/– <––> RX/Ring/–
5	2	TX/Tip/+ <––> RX/Tip/+
3	3	Shield/Return/Ground
6	6	Shield/Return/Ground
7	No connect	No connect
8	No connect	No connect

Table 64: RJ-48 Connector to DB-15 Connector (Straight) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data numbering form)	DB-15 Pin (Data numbering form)	Signal
1	11	RX/Ring/– <––> RX/Ring/–
2	3	RX/Tip/+ <––> RX/Tip/+
4	9	TX/Ring/– <––> TX/Ring/–
5	1	TX/Tip/+ <––> TX/Tip/+
3	4	Shield/Return/Ground
6	2	Shield/Return/Ground
7	No connect	No connect
8	No connect	No connect
9	No connect	No connect
10	No connect	No connect

Table 64: RJ-48 Connector to DB-15 Connector (Straight) Pinout (continued)

RJ-48 Pin (on T1/E1 PIM) (Data numbering form)	DB-15 Pin (Data numbering form)	Signal
11	No connect	No connect
12	No connect	No connect
13	No connect	No connect
14	No connect	No connect
15	No connect	No connect

Table 65: RJ-48 Connector to DB-15 Connector (Crossover) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data numbering form)	DB-15 Pin (Data numbering form)	Signal
1	9	RX/Ring/– <––> TX/Ring/–
2	1	RX/Tip/+ <––> TX/Tip/+
4	11	TX/Ring/– <––> RX/Ring/–
5	3	TX/Tip/+ <––> RX/Tip/+
3	4	Shield/Return/Ground
6	2	Shield/Return/Ground
7	No connect	No connect
8	No connect	No connect
9	No connect	No connect
10	No connect	No connect
11	No connect	No connect
12	No connect	No connect
13	No connect	No connect
14	No connect	No connect
15	No connect	No connect

E3 and T3 BNC Connector Pinout

The E3 and T3 PIMs each use two BNC connectors—one for transmitting data (TX) and one for receiving data (RX).

ADSL and G.SHDSL RJ-11 Connector Pinout

The 1-port ADSL 2/2+ Annex A and Annex B PIMs use an RJ-11 cable, which is not supplied with the PIMs. The 2-port G.SHDSL Annex A and Annex B PIM also uses an RJ-11 cable, which is not supplied with the PIM. Table 66 describes the RJ-11 connector pinout.

Table 66: ADSL and G.SHDSL RJ-11 Connector Pinout

Pin	Signal
1	No connect
2	No connect
3	RJ P –Tip
4	RJ N –Ring
5	No connect
6	No connect

ISDN RJ-45 Connector Pinout

The 1-port and 4-port ISDN PIMs use an RJ-45 cable, which is not supplied with the PIMs. Table 67 describes the RJ-45 connector pinout.

Table 67: ISDN RJ-45 Connector Pinout

Pin	Signal
1	No connect
2	No connect
3	RJ_SX_P
4	RJ_SR_P
5	RJ_SR_N
6	RJ_SX_N
7	No connect
8	No connect
9	Shielded
10	Shielded 2

Chapter 14

Safety and Regulatory Compliance Information

To install and use the Services Router safely, follow proper safety procedures. This chapter discusses the following safety and regulatory compliance information:

- Definition of Safety Warning Levels on page 201
- Safety Guidelines and Warnings on page 203
- Agency Approvals on page 240
- Compliance Statements for Environmental Requirements on page 241
- Compliance Statements for EMC Requirements on page 241
- Product Reclamation and Recycling Program on page 246

Definition of Safety Warning Levels

This manual uses the following three levels of safety warnings:

NOTE: You might find this information helpful in a particular situation, or might otherwise overlook it.

CAUTION: You need to observe the specified guidelines to avoid minor injury or discomfort to you, or severe damage to the Services Router.

WARNING: This symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

WARNING: Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

WARNING: Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

WARNING: Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

WARNING: Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

WARNING: Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

WARNING: Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

WARNING: Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

WARNING: ¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

WARNING: Varning! Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

Safety Guidelines and Warnings

This section lists the following safety guidelines and warnings for installing, operating, and maintaining a Services Router:

- General Safety Guidelines and Warnings on page 203
- Electrical Safety Guidelines and Warnings on page 206
- Installation Safety Guidelines and Warnings on page 221
- Laser and LED Safety Guidelines and Warnings on page 227
- Maintenance and Operational Safety Guidelines and Warnings on page 231

General Safety Guidelines and Warnings

The following guidelines help ensure your safety and protect the Services Router from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in this manual. Make sure that only authorized service personnel perform other system services.

- Keep the area around the chassis clear and free from dust before, during, and after installation.
- Keep tools away from areas where people could trip over them while walking.
- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the chassis.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.
- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the Services Router only when it is properly grounded.
- The separate protective earthing terminal provided on this product shall be permanently connected to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet metal parts unless instructions are provided in this manual. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the Services Router chassis or onto any Services Router component. Such an action could cause electrical shock or damage the Services Router.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.

In addition, observe the warnings and guidelines in the following sections.

Qualified Personnel Warning

WARNING: Only trained and qualified personnel should install or replace the Services Router.

Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

Varoitus Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.

Attention Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.

Warnung Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.

WARNING: Avvertenza Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.

Advarsel Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.

Aviso Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.

¡Atención! Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.

Varning! Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

Preventing Electrostatic Discharge Damage

Many Services Router hardware components are sensitive to damage from static electricity. Some components can be impaired by voltages as low as 30 V. You can easily generate potentially damaging static voltages whenever you handle plastic or foam packing material or if you move components across plastic or carpets. Observe the following guidelines to minimize the potential for electrostatic discharge (ESD) damage, which can cause intermittent or complete component failures:

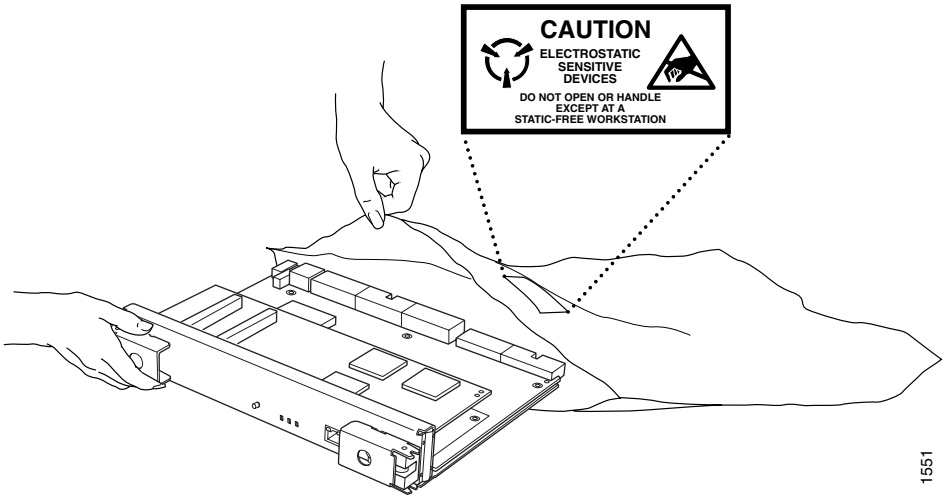
- Always use an ESD wrist strap or ankle strap, and make sure that it is in direct contact with your skin.

CAUTION: For safety, periodically check the resistance value of the ESD strap. The measurement should be in the range of 1 to 10 Mohms.

- When handling any component that is removed from the chassis, make sure the equipment end of your ESD strap is attached to one of the electrostatic discharge points on the chassis, which are shown in Figure 2 .

- Avoid contact between the component and your clothing. ESD voltages emitted from clothing can still damage components.
- When removing or installing a component, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an electrostatic bag (see Figure 57). If you are returning a component, place it in an electrostatic bag before packing it.

Figure 57: Place a Component into an Electrostatic Bag



Electrical Safety Guidelines and Warnings

When working on equipment powered by electricity, follow the guidelines described in the following sections:

- General Electrical Safety Guidelines on page 207
- AC Power Electrical Safety Guidelines on page 208
- DC Power Electrical Safety Guidelines on page 209
- Power Sources for Redundant Power Supplies on page 209
- DC Power Disconnection Warning on page 210
- DC Power Grounding Requirements and Warning on page 211
- DC Power Wiring Sequence Warning on page 212
- DC Power Wiring Terminations Warning on page 213
- Grounded Equipment Warning on page 214

- Warning Statement for Norway and Sweden on page 215
- In Case of Electrical Accident on page 215
- Multiple Power Supplies Disconnection Warning on page 215
- Power Disconnection Warning on page 217
- TN Power Warning on page 218
- Telecommunication Line Cord Warning on page 219

General Electrical Safety Guidelines

- Install the Services Router in compliance with the following local, national, or international electrical codes:
  - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code.
  - Canada—Canadian Electrical Code, Part 1, CSA C22.1.
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7.
  - Evaluated to the TN power system.
- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.
- Operate the Services Router within marked electrical ratings and product usage instructions.
- For the Services Router and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

Many Services Router components can be removed and replaced without powering down or disconnecting power to the Services Router, as detailed in elsewhere in this manual. Never install equipment if it appears damaged.

AC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to AC-powered routers:

- AC-powered routers are shipped with a three-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding should comply with local and national electrical codes.
- You must provide an external Listed circuit breaker rated minimum 15 A in the building installation.
- The power cord serves as the main disconnecting device. The socket outlet must be near the router and be easily accessible.
- The cores in the mains lead are colored in accordance with the following code:
  - Green and yellow—Earth
  - Blue—Neutral
  - Brown—Live
- When a router is equipped with two AC power supplies, both power cords (one for each power supply) must be unplugged to completely disconnect power to the router.
- Note the following warnings printed on the AC power supply faceplate:
  - To completely de-energize the system disconnect maximum of 2 power cordsets.
  - Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk. [Swedish]

Power Cable Warning (Japanese)

WARNING: The attached power cable is only for this product. Do not use the cable for another product.

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

g017253

DC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to a DC-powered router:

- A DC-powered router is equipped with a DC terminal block that is rated for the power requirements of a maximally configured router. To supply sufficient power, terminate the DC input wiring on a facility DC source capable of supplying at least 8 A @ –48 VDC. Incorporate an easily accessible disconnect device into the facility wiring. Be sure to connect the ground wire or conduit to a solid office (earth) ground. A closed loop ring is recommended for terminating the ground conductor at the ground stud.
- Run two wires from the circuit breaker box to a source of 48 VDC.
- In the United States, a restricted access area is one in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code ANSI/NFPA 70.

NOTE: Primary overcurrent protection is provided by the building circuit breaker. This breaker should protect against excess currents, short circuits, and earth faults in accordance with NEC ANSI/NFPA70.

- Ensure that the polarity of the DC input wiring is correct. Under certain conditions, connections with reversed polarity might trip the primary circuit breaker or damage the equipment.
- For personal safety, connect the green and yellow wire to safety (earth) ground at both the router and the supply side of the DC wiring.
- The marked input voltage of –48 VDC for a DC-powered router is the nominal voltage associated with the battery circuit, and any higher voltages are only to be associated with float voltages for the charging function.
- Because the router is a positive ground system, you must connect the positive lead to the terminal labeled RTN, the negative lead to the terminal labeled –48 VDC, and the earth ground to the chassis grounding points.

Power Sources for Redundant Power Supplies

If your J6350 Services Router includes an optional redundant DC power supply, connect each of the two power supplies to different input power sources. Failure to do so makes the router susceptible to total power failure if one of the power supplies fails.

ђ ћ

JuniperNetworks ъ У э Л ђ ћ ч э Ї a ь ю
. a m JuniperNetworks У k ѕ .

DC Power Disconnection Warning

WARNING: Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

Waarschuwing Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

Varoitus Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.

Attention Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.

Warnung Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.

Avvertenza Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.

Advarsel Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.

Aviso Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.

¡Atención! Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para

asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).

Varning! Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.

DC Power Grounding Requirements and Warning

An insulated grounding conductor that is identical in size to the grounded and ungrounded branch circuit supply conductors, but is identifiable by green and yellow stripes, is installed as part of the branch circuit that supplies the unit. The grounding conductor is a separately derived system at the supply transformer or motor generator set.

For further information, see "Chassis Grounding" on page 86 and "DC Power, Connection, and Power Cable Specifications" on page 77.

WARNING: When installing the router, the ground connection must always be made first and disconnected last.

Waarschuwing Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.

Varoitus Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.

Attention Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.

Warnung Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.

Avvertenza In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.

Advarsel Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.

Aviso Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.

¡Atención! Al instalar el equipo, conectar la tierra la primera y desconectarla la última.

Varning! Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.

DC Power Wiring Sequence Warning

WARNING: Wire the DC power supply using the appropriate lugs. When connecting power, the proper wiring sequence is ground to ground, + RTN to + RTN, then -48 V to -48 V. When disconnecting power, the proper wiring sequence is -48 V to -48 V, + RTN to + RTN, then ground to ground. Note that the ground wire should always be connected first and disconnected last.

Waarschuwing De juiste bedradingsvolgorde verbonden is aarde naar aarde, + RTN naar + RTN, en –48 V naar – 48 V. De juiste bedradingsvolgorde losgemaakt is en –48 V naar – 48 V, + RTN naar + RTN, aarde naar aarde.

Varoitus Oikea yhdistettava kytkentajarjestys on maajohto maajohtoon, + RTN varten + RTN, –48 V varten – 48 V. Oikea irrotettava kytkentajarjestys on –48 V varten – 48 V, + RTN varten + RTN, maajohto maajohtoon.

Attention Câblez l'approvisionnement d'alimentation CC En utilisant les crochets appropriés à l'extrémité de câblage. En reliant la puissance, l'ordre approprié de câblage est rectifié pour rectifier, + RTN à + RTN, puis -48 V à -48 V. En débranchant la puissance, l'ordre approprié de câblage est -48 V à -48 V, + RTN à + RTN, a alors rectifié pour rectifier. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois.

Warnung Verdrahten Sie die Gleichstrom-Versorgung mit den passenden Ansätzen am Verdrahtung Ende. Wenn man Energie anschließt, wird die korrekte Verdrahtung. Reihenfolge gerieben, um, + RTN zu + RTN, dann -48 V bis -48 V zu reiben. Wenn sie Energie trennt, ist die korrekte Verdrahtung Reihenfolge -48 V bis -48 V, + RTN zu + RTN, rieb dann, um zu reiben. Beachten Sie, daß der Erdungsdraht immer zuerst angeschlossen werden und zuletzt getrennt werden sollte.

Avvertenza Mostra la morsettiera dell alimentatore CC. Cablare l'alimentatore CC usando i connettori adatti all'estremità del cablaggio, come illustrato. La corretta sequenza di cablaggio è da massa a massa, da positivo a positivo (da linea ad L) e da negativo a negativo (da neutro a N). Tenere presente che il filo di massa deve sempre venire collegato per primo e scollegato per ultimo.

Advarsel Riktig tilkoples tilkoplingssekvens er jord til jord, + RTN til + RTN, –48 V til – 48 V. Riktig frakoples tilkoplingssekvens er –48 V til – 48 V, + RTN til + RTN, jord til jord.

Aviso Ate con alambre la fuente de potencia cc Usando los terminales apropiados en el extremo del cableado. Al conectar potencia, la secuencia apropiada del cableado se muele para moler, + RTN a + RTN, entonces -48 V a -48 V. Al desconectar potencia, la secuencia apropiada del cableado es -48 V a -48 V, + RTN

a + RTN, entonces molió para moler. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último.

¡Atención! Wire a fonte de alimentação de DC Usando os talões apropriados na extremidade da fiação. Ao conectar a potência, a seqüência apropriada da fiação é moída para moer, + RTN a + RTN, então -48 V a -48 V. Ao desconectar a potência, a seqüência apropriada da fiação é -48 V a -48 V, + RTN a + RTN, moeu então para moer. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último.

Varning! Korrekt kopplingssekvens ar jord till jord, + RTN till + RTN, –48 V till – 48 V. Korrekt kopplas kopplingssekvens ar –48 V till – 48 V, + RTN till + RTN, jord till jord.

DC Power Wiring Terminations Warning

WARNING: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.

Waarschuwing Wanneer geslagen bedrading vereist is, dient u bedrading te gebruiken die voorzien is van goedgekeurde aansluitingspunten, zoals het gesloten-lus type of het grijperschop type waarbij de aansluitpunten omhoog wijzen. Deze aansluitpunten dienen de juiste maat voor de draden te hebben en dienen zowel de isolatie als de geleider vast te klemmen.

Varoitus Jos säikeellinen johdin on tarpeen, käytä hyväksyttyä johdinliitäntää, esimerkiksi suljettua silmukkaa tai kourumaista liitäntää, jossa on ylöspäin käännetyt kiinnityskorvat. Tällaisten liitäntöjen tulee olla kooltaan johtimiin sopivia ja niiden tulee puristaa yhteen sekä eristeen että johdinosan.

Attention Quand des fils torsadés sont nécessaires, utiliser des douilles terminales homologuées telles que celles à circuit fermé ou du type à plage ouverte avec cosses rebroussées. Ces douilles terminales doivent être de la taille qui convient aux fils et doivent être refermées sur la gaine isolante et sur le conducteur.

Warnung Wenn Litzenverdrahtung erforderlich ist, sind zugelassene Verdrahtungsabschlüsse, z.B. für einen geschlossenen Regelkreis oder gabelförmig, mit nach oben gerichteten Kabelschuhen zu verwenden. Diese Abschlüsse sollten die angemessene Größe für die Drähte haben und sowohl die Isolierung als auch den Leiter festklemmen.

Avvertenza Quando occorre usare trecce, usare connettori omologati, come quelli a occhiello o a forcella con linguette rivolte verso l'alto. I connettori devono avere la misura adatta per il cablaggio e devono serrare sia l'isolante che il conduttore.

Advarsel Hvis det er nødvendig med flertrådede ledninger, brukes godkjente ledningsavslutninger, som for eksempel lukket sløyfe eller spadetype med oppoverbøyde kabelsko. Disse avslutningene skal ha riktig størrelse i forhold til ledningene, og skal klemme sammen både isolasjonen og lederen.

Aviso Quando forem requeridas montagens de instalação eléctrica de cabo torcido, use terminações de cabo aprovadas, tais como, terminações de cabo em circuito fechado e planas com terminais de orelha voltados para cima. Estas terminações de cabo deverão ser do tamanho apropriado para os respectivos cabos, e deverão prender simultaneamente o isolamento e o fio condutor.

¡Atención! Cuando se necesite hilo trenzado, utilizar terminales para cables homologados, tales como las de tipo "bucle cerrado" o "espada", con las lengüetas de conexión vueltas hacia arriba. Estos terminales deberán ser del tamaño apropiado para los cables que se utilicen, y tendrán que sujetar tanto el aislante como el conductor.

Varning! När flertrådiga ledningar krävs måste godkända ledningskontakter användas, t.ex. kabelsko av sluten eller öppen typ med uppåtvänd tapp. Storleken på dessa kontakter måste vara avpassad till ledningarna och måste kunna hålla både isoleringen och ledaren fastklämda.

Grounded Equipment Warning

WARNING: The router is intended to be grounded. Ensure that the router is connected to earth ground during normal use.

Waarschuwing Deze apparatuur hoort geaard te worden Zorg dat de host-computer tijdens normaal gebruik met aarde is verbonden.

Varoitus Tämä laitteisto on tarkoitettu maadoitettavaksi. Varmista, että isäntälaite on yhdistetty maahan normaalikäytön aikana.

Attention Cet équipement doit être relié à la terre. S'assurer que l'appareil hôte est relié à la terre lors de l'utilisation normale.

Warnung Dieses Gerät muß geerdet werden. Stellen Sie sicher, daß das Host-Gerät während des normalen Betriebs an Erde gelegt ist.

WARNING: Avvertenza Questa apparecchiatura deve essere collegata a massa. Accertarsi che il dispositivo host sia collegato alla massa di terra durante il normale utilizzo.

Advarsel Dette utstyret skal jordes. Forviss deg om vertsterminalen er jordet ved normalt bruk.

Aviso Este equipamento deverá estar ligado à terra. Certifique-se que o host se encontra ligado à terra durante a sua utilização normal.

¡Atención! Este equipo debe conectarse a tierra. Asegurarse de que el equipo principal esté conectado a tierra durante el uso normal.

Varning! Denna utrustning är avsedd att jordas. Se till att värdenheten är jordad vid normal användning.

Warning Statement for Norway and Sweden

WARNING: The equipment must be connected to an earthed mains socket-outlet.

Advarsel Apparatet skal kobles til en jordet stikkontakt.

Varning! Apparaten skall anslutas till jordat nätuttag.

In Case of Electrical Accident

If an electrical accident results in an injury, take the following actions in this order:

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.
2. Disconnect power from the Services Router.
3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, then call for help.

Multiple Power Supplies Disconnection Warning

WARNING: The J6350 Services Router has more than one power supply connection. All connections must be removed completely to remove power from the unit completely.

WARNING: Waarschuwing Deze J6350 eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.

WARNING: Varoitus Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.

WARNING: Attention Cette J6350 unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.

WARNING: Warnung Diese J6350 Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.

WARNING: Avvertenza Questa J6350 unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.

WARNING: Advarsel Denne J6350 enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.

WARNING: Aviso Este J6350 dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.

WARNING: ¡Atención! Esta J6350 unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.

WARNING: Varning! Denna J6350 enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.

Power Disconnection Warning

WARNING: Before working on the router or near power supplies, unplug the power cord from an AC router.

WARNING: Waarschuwing Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen.

WARNING: Varoitus Kytke irti vaihtovirtalaitteiden virtajohto, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.

WARNING: Attention Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif.

WARNING: Warnung Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw.

WARNING: Avvertenza Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA.

WARNING: Advarsel Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter.

WARNING: Aviso Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada.

WARNING: ¡Atención! Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA).

WARNING: Varning! Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden.

TN Power Warning

WARNING: The router is designed to work with a TN power system.

WARNING: Waarschuwing Het apparaat is ontworpen om te functioneren met TN energiesystemen.

WARNING: Varoitus Koje on suunniteltu toimimaan TN-sähkövoimajärjestelmien yhteydessä.

WARNING: Attention Ce dispositif a été conçu pour fonctionner avec des systèmes d'alimentation TN.

WARNING: Warnung Das Gerät ist für die Verwendung mit TN-Stromsystemen ausgelegt.

WARNING: Avvertenza Il dispositivo è stato progettato per l'uso con sistemi di alimentazione TN.

WARNING: Advarsel Utstyret er utfomet til bruk med TN-strømsystemer.

WARNING: Aviso O dispositivo foi criado para operar com sistemas de corrente TN.

WARNING: ¡Atención! El equipo está diseñado para trabajar con sistemas de alimentación tipo TN.

WARNING: Varning! Enheten är konstruerad för användning tillsammans med elkraftssystem av TN-typ.

Telecommunication Line Cord Warning

WARNING: To reduce the risk of fire, use only No. 26 AWG or larger UL-listed or CSA-certified telecommunication line cord.

WARNING: Waarschuwing Om brandgevaar te reduceren, dient slechts telecommunicatielijnsnoer nr. 26 AWG of groter gebruikt te worden.

WARNING: Varoitus Tulipalovaaran vähentämiseksi käytä ainoastaan nro 26 AWG- tai paksumpaa tietoliikennejohdinta.

WARNING: Attention Pour réduire les risques d'incendie, n'utiliser que des cordons de lignes de télécommunications de type AWG n° 26 ou plus larges.

WARNING: Warnung Zur Reduzierung der Feuergefahr eine Fernmeldeleitungsschnur der Größe 26 AWG oder größer verwenden.

WARNING: Avvertenza Per ridurre il rischio di incendio, usare solo un cavo per linea di telecomunicazioni di sezione 0,12 mm2 (26 AWG) o maggiore.

WARNING: Advarsel Bruk kun AWG nr. 26 eller telekommunikasjonsledninger med større dimensjon for å redusere faren for brann.

WARNING: Aviso Para reduzir o risco de incêndio, utilize apenas terminais de fio de telecomunicações Nº. 26 AWG ou superiores.

WARNING: ¡Atención! Para reducir el riesgo de incendios, usar sólo líneas de telecomunicaciones de calibre No. 26 AWG o más gruesas.

WARNING: Varning! För att minska brandrisken skall endast Nr. 26 AWG eller större telekommunikationsledning användas.

Installation Safety Guidelines and Warnings

Observe the following guidelines and warnings before and during Services Router installation:

- Chassis Lifting Guidelines on page 221
- Installation Instructions Warning on page 221
- Rack-Mounting Requirements and Warnings on page 222
- Ramp Warning on page 226

Chassis Lifting Guidelines

The weight of a fully populated chassis is approximately 25.3 lbs (11.5 kg) for a J4350 Services Router, and 30.7 lb (13.9 kg) for a J6350 Services Router. Observe the following guidelines for lifting and moving a Services Router:

- Before moving the Services Router, read the guidelines in "Preparing for Router Installation" on page 71 to verify that the intended site meets the specified power, environmental, and clearance requirements.
- Before lifting or moving the Services Router, disconnect all external cables.
- As when lifting any heavy object, lift most of the weight with your legs rather than your back. Keep your knees bent and your back relatively straight and avoid twisting your body as you lift. Balance the load evenly and be sure that your footing is solid.

Installation Instructions Warning

WARNING: Read the installation instructions before you connect the router to a power source.

Waarschuwing Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.

Varoitus Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

Attention Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

Warnung Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.

WARNING: Avvertenza Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

Advarsel Les installasjonsinstruksjonene før systemet kobles til strømkilden.

Aviso Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.

¡Atención! Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Varning! Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

Rack-Mounting Requirements and Warnings

Ensure that the equipment rack into which the Services Router is installed is evenly and securely supported, to avoid the hazardous condition that could result from uneven mechanical loading.

WARNING: To prevent bodily injury when mounting or servicing the router in a rack, take the following precautions to ensure that the system remains stable. The following directives help maintain your safety:

- The router must be installed into a rack that is secured to the building structure.
- The router should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting the router in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the router in the rack.

WARNING: Waarschuwing Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale

voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:

- De Juniper Networks router moet in een stellage worden geïnstalleerd die aan een bouwsel is verankerd.
- Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.
- Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.
- Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.

WARNING: Varoitus Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:

- Juniper Networks router on asennettava telineeseen, joka on kiinnitetty rakennukseen.
- Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.
- Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.
- Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.

WARNING: Attention Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel:

- Le rack sur lequel est monté le Juniper Networks router doit être fixé à la structure du bâtiment.
- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.

- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.
- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

WARNING: Warnung Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:

- Der Juniper Networks router muß in einem Gestell installiert werden, das in der Gebäudestruktur verankert ist.
- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.
- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.
- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

WARNING: Avvertenza Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:

- Il Juniper Networks router deve essere installato in un telaio, il quale deve essere fissato alla struttura dell'edificio.
- Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.
- Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.
- Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.

WARNING: Advarsel Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:

- Juniper Networks router må installeres i et stativ som er forankret til bygningsstrukturen.
- Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.
- Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.
- Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.

WARNING: Aviso Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:

- O Juniper Networks router deverá ser instalado numa prateleira fixa à estrutura do edificio.
- Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.
- Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.
- Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.

WARNING: ¡Atención! Para evitar lesiones durante el montaje de este equipo sobre un bastidor, o posteriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:

- El Juniper Networks router debe instalarse en un bastidor fijado a la estructura del edificio.
- Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.

- Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.
- Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.

WARNING: Varning! För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:

- Juniper Networks router måste installeras i en ställning som är förankrad i byggnadens struktur.
- Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.
- Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.
- Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.

Ramp Warning

WARNING: When installing the router, do not use a ramp inclined at more than 10 degrees.

Waarschuwing Gebruik een oprijplaat niet onder een hoek van meer dan 10 graden.

Varoitus Älä käytä sellaista kaltevaa pintaa, jonka kaltevuus ylittää 10 astetta.

Attention Ne pas utiliser une rampe dont l'inclinaison est supérieure à 10 degrés.

Warnung Keine Rampen mit einer Neigung von mehr als 10 Grad verwenden.

WARNING: Avvertenza Non usare una rampa con pendenza superiore a 10 gradi.

Advarsel Bruk aldri en rampe som heller mer enn 10 grader.

Aviso Não utilize uma rampa com uma inclinação superior a 10 graus.

¡Atención! No usar una rampa inclinada más de 10 grados

Varning! Använd inte ramp med en lutning på mer än 10 grader.

Laser and LED Safety Guidelines and Warnings

Single-mode Physical Interface Modules (PIMs) are equipped with laser transmitters, which are considered a Class 1 Laser Product by the U.S. Food and Drug Administration, and are evaluated as a Class 1 Laser Product per EN 60825–1 + A11 + A2 requirements.

Observe the following guidelines and warnings:

- General Laser Safety Guidelines on page 227
- Class 1 Laser Product Warning on page 227
- Class 1 LED Product Warning on page 228
- Laser Beam Warning on page 229
- Radiation from Open Port Apertures Warning on page 230

General Laser Safety Guidelines

When working around PIMs, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.

WARNING: Unterminated optical connectors can emit invisible laser radiation. The lens in the human eye focuses all the laser power on the retina, so focusing the eye directly on a laser source—even a low-power laser—could permanently damage the eye.

Class 1 Laser Product Warning

WARNING: Class 1 laser product.

Waarschuwing Klasse-1 laser produkt.

Varoitus Luokan 1 lasertuote.

Attention Produit laser de classe I.

Warnung Laserprodukt der Klasse 1.

WARNING: Avvertenza Prodotto laser di Classe 1.

Advarsel Laserprodukt av klasse 1.

Aviso Produto laser de classe 1.

¡Atención! Producto láser Clase I.

Varning! Laserprodukt av klass 1.

Class 1 LED Product Warning

WARNING: Class 1 LED product.

Waarschuwing Klasse 1 LED-product.

Varoitus Luokan 1 valodiodituote.

Attention Alarme de produit LED Class I.

Warnung Class 1 LED-Produktwarnung.

WARNING: Avvertenza Avvertenza prodotto LED di Classe 1.

Advarsel LED-produkt i klasse 1.

Aviso Produto de classe 1 com LED.

¡Atención! Aviso sobre producto LED de Clase 1.

Varning! Lysdiodprodukt av klass 1.

Laser Beam Warning

WARNING: Do not stare into the laser beam or view it directly with optical instruments.

WARNING: Waarschuwing Niet in de straal staren of hem rechtstreeks bekijken met optische instrumenten.

WARNING: Varoitus Älä katso säteeseen äläkä tarkastele sitä suoraan optisen laitteen avulla.

WARNING: Attention Ne pas fixer le faisceau des yeux, ni l'observer directement à l'aide d'instruments optiques.

WARNING: Warnung Nicht direkt in den Strahl blicken und ihn nicht direkt mit optischen Geräten prüfen.

WARNING: Avvertenza Non fissare il raggio con gli occhi né usare strumenti ottici per osservarlo direttamente.

WARNING: Advarsel Stirr eller se ikke direkte p strlen med optiske instrumenter.

WARNING: Aviso Não olhe fixamente para o raio, nem olhe para ele directamente com instrumentos ópticos.

WARNING: ¡Atención! No mirar fijamente el haz ni observarlo directamente con instrumentos ópticos.

WARNING: Varning! Rikta inte blicken in mot strålen och titta inte direkt på den genom optiska instrument.

Radiation from Open Port Apertures Warning

WARNING: Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.

WARNING: Waarschuwing Aangezien onzichtbare straling vanuit de opening van de poort kan komen als er geen fiberkabel aangesloten is, dient blootstelling aan straling en het kijken in open openingen vermeden te worden.

WARNING: Varoitus Koska portin aukosta voi emittoitua näkymätöntä säteilyä, kun kuitukaapelia ei ole kytkettynä, vältä säteilylle altistumista äläkä katso avoimiin aukkoihin.

WARNING: Attention Des radiations invisibles à l'il nu pouvant traverser l'ouverture du port lorsqu'aucun câble en fibre optique n'y est connecté, il est recommandé de ne pas regarder fixement l'intérieur de ces ouvertures.

WARNING: Warnung Aus der Port-Öffnung können unsichtbare Strahlen emittieren, wenn kein Glasfaserkabel angeschlossen ist. Vermeiden Sie es, sich den Strahlungen auszusetzen, und starren Sie nicht in die Öffnungen!

WARNING: Avvertenza Quando i cavi in fibra non sono inseriti, radiazioni invisibili possono essere emesse attraverso l'apertura della porta. Evitate di esporvi alle radiazioni e non guardate direttamente nelle aperture.

WARNING: Advarsel Unngå utsettelse for stråling, og stirr ikke inn i åpninger som er åpne, fordi usynlig stråling kan emiteres fra portens åpning når det ikke er tilkoblet en fiberkabel.

WARNING: Aviso Dada a possibilidade de emissão de radiação invisível através do orifício da via de acesso, quando esta não tiver nenhum cabo de fibra conectado, deverá evitar a exposição à radiação e não deverá olhar fixamente para orifícios que se encontrarem a descoberto.

WARNING: ¡Atención! Debido a que la apertura del puerto puede emitir radiación invisible cuando no existe un cable de fibra conectado, evite mirar directamente a las aperturas para no exponerse a la radiación.

WARNING: Varning! Osynlig strålning kan avges från en portöppning utan ansluten fiberkabel och du bör därför undvika att bli utsatt för strålning genom att inte stirra in i oskyddade öppningar.

Maintenance and Operational Safety Guidelines and Warnings

As you maintain the Services Router, observe the following guidelines and warnings:

- Battery Handling Warning on page 232
- Jewelry Removal Warning on page 233
- Lightning Activity Warning on page 235
- Operating Temperature Warning on page 236
- Product Disposal Warning on page 238

Battery Handling Warning

WARNING: Replacing the battery incorrectly might result in an explosion. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

WARNING: Waarschuwing Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.

WARNING: Varoitus Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.

WARNING: Attention Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

WARNING: Warnung Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

WARNING: Advarsel Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.

WARNING: Avvertenza Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.

WARNING: Aviso Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.

WARNING: ¡Atención! Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

WARNING: Varning! Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

Jewelry Removal Warning

WARNING: Before working on equipment that is connected to power lines, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

WARNING: Waarschuwing Alvorens aan apparatuur te werken die met elektrische leidingen is verbonden, sieraden (inclusief ringen, kettingen en horloges) verwijderen. Metalen voorwerpen worden warm wanneer ze met stroom en aarde zijn verbonden, en kunnen ernstige brandwonden veroorzaken of het metalen voorwerp aan de aansluitklemmen lassen.

WARNING: Varoitus Ennen kuin työskentelet voimavirtajohtoihin kytkettyjen laitteiden parissa, ota pois kaikki korut (sormukset, kaulakorut ja kellot mukaan lukien). Metalliesineet kuumenevat, kun ne ovat yhteydessä sähkövirran ja maan kanssa, ja ne voivat aiheuttaa vakavia palovammoja tai hitsata metalliesineet kiinni liitäntänapoihin.

WARNING: Attention Avant d'accéder à cet équipement connecté aux lignes électriques, ôter tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

WARNING: Warnung Vor der Arbeit an Geräten, die an das Netz angeschlossen sind, jeglichen Schmuck (einschließlich Ringe, Ketten und Uhren) abnehmen. Metallgegenstände erhitzen sich, wenn sie an das Netz und die Erde angeschlossen werden, und können schwere Verbrennungen verursachen oder an die Anschlußklemmen angeschweißt werden.

WARNING: Avvertenza Prima di intervenire su apparecchiature collegate alle linee di alimentazione, togliersi qualsiasi monile (inclusi anelli, collane, braccialetti ed orologi). Gli oggetti metallici si riscaldano quando sono collegati tra punti di alimentazione e massa: possono causare ustioni gravi oppure il metallo può saldarsi ai terminali.

WARNING: Advarsel Fjern alle smykker (inkludert ringer, halskjeder og klokker) før du skal arbeide på utstyr som er koblet til kraftledninger. Metallgjenstander som er koblet til kraftledninger og jord blir svært varme og kan forårsake alvorlige brannskader eller smelte fast til polene.

WARNING: Aviso Antes de trabalhar em equipamento que esteja ligado a linhas de corrente, retire todas as jóias que estiver a usar (incluindo anéis, fios e relógios). Os objectos metálicos aquecerão em contacto com a corrente e em contacto com

a ligação à terra, podendo causar queimaduras graves ou ficarem soldados aos terminais.

WARNING: ¡Atención! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

WARNING: Varning! Tag av alla smycken (inklusive ringar, halsband och armbandsur) innan du arbetar på utrustning som är kopplad till kraftledningar. Metallobjekt hettas upp när de kopplas ihop med ström och jord och kan förorsaka allvarliga brännskador; metallobjekt kan också sammansvetsas med kontakterna.

Lightning Activity Warning

WARNING: Do not work on the system or connect or disconnect cables during periods of lightning activity.

WARNING: Waarschuwing Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.

WARNING: Varoitus Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

WARNING: Attention Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

WARNING: Warnung Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

WARNING: Avvertenza Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

WARNING: Advarsel Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

WARNING: Aviso Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

WARNING: ¡Atención! No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

WARNING: Varning! Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

Operating Temperature Warning

WARNING: To prevent the router from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C). To prevent airflow restriction, allow at least 6 inches (15.2 cm) of clearance around the ventilation openings.

WARNING: Waarschuwing Om te voorkomen dat welke router van de Juniper Networks router dan ook oververhit raakt, dient u deze niet te bedienen op een plaats waar de maximale aanbevolen omgevingstemperatuur van 40°C wordt overschreden. Om te voorkomen dat de luchtstroom wordt beperkt, dient er minstens 15,2 cm speling rond de ventilatie-openingen te zijn.

WARNING: Varoitus Ettei Juniper Networks router-sarjan reititin ylikuumentuisi, sitä ei saa käyttää tilassa, jonka lämpötila ylittää korkeimman suositellun ympäristölämpötilan 40°C. Ettei ilmanvaihto estyisi, tuuletusaukkojen ympärille on jätettävä ainakin 15,2 cm tilaa.

WARNING: Attention Pour éviter toute surchauffe des routeurs de la gamme Juniper Networks router, ne l'utilisez pas dans une zone où la température ambiante est supérieure à 40°C. Pour permettre un flot d'air constant, dégagez un espace d'au moins 15,2 cm autour des ouvertures de ventilations.

WARNING: Warnung Um einen Router der router vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene Maximum von 40°C überschreitet. Um Lüftungsverschluß zu verhindern, achten Sie darauf, daß mindestens 15,2 cm lichter Raum um die Lüftungsöffnungen herum frei bleibt.

WARNING: Avvertenza Per evitare il surriscaldamento dei router, non adoperateli in un locale che ecceda la temperatura ambientale massima di 40°C. Per evitare che la circolazione dell'aria sia impedita, lasciate uno spazio di almeno 15.2 cm di fronte alle aperture delle ventole.

WARNING: Advarsel Unngå overoppheting av eventuelle rutere i Juniper Networks router Disse skal ikke brukes på steder der den anbefalte maksimale omgivelsestemperaturen overstiger 40°C (104°F). Sørg for at klaringen rundt lufteåpningene er minst 15,2 cm (6 tommer) for å forhindre nedsatt luftsirkulasjon.

WARNING: Aviso Para evitar o sobreaquecimento do encaminhador Juniper Networks router, não utilize este equipamento numa área que exceda a temperatura máxima recomendada de 40°C. Para evitar a restrição à circulação de ar, deixe pelo menos um espaço de 15,2 cm à volta das aberturas de ventilação.

WARNING: ¡Atención! Para impedir que un encaminador de la serie Juniper Networks router se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40°C. Para impedir la restricción de la entrada de aire, deje un espacio mínimo de 15,2 cm alrededor de las aperturas para ventilación.

WARNING: Varning! Förhindra att en Juniper Networks router överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40°C överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.

Product Disposal Warning

WARNING: Disposal of this product must be handled according to all national laws and regulations.

WARNING: Waarschuwing Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

WARNING: Varoitus Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

WARNING: Attention La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

WARNING: Warnung Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.

WARNING: Avvertenza L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia

WARNING: Advarsel Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

WARNING: Aviso A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

WARNING: ¡Atención! El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales

WARNING: Varning! Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

Agency Approvals

The Services Router complies with the following standards:

- Safety
  - CAN/CSA-22.2 No. 60950–1–03–UL 60950–1 Safety of Information Technology Equipment
  - EN 60950–1 Safety of Information Technology Equipment
  - EN 60825-1 Safety of Laser Products - Part 1: Equipment Classification, Requirements and User's Guide
- EMC
  - AS/NZS 3548 Class B (Australia/New Zealand)
  - EN 55022 Class B Emissions (Europe)
  - FCC Part 15 Class B (USA)
  - VCCI Class B (Japan)
  - FCC Part 68
  - Industry Canada CS-03
- Immunity
  - EN 61000-3-2 Power Line Harmonics
  - EN 61000-3-3 Voltage Fluctuations and Flicker
  - EN 61000-4-2 ESD
  - EN 61000-4-3 Radiated Immunity
  - EN 61000-4-4 EFT
  - EN 61000-4-5 Surge
  - EN 61000-4-6 Low Frequency Common Immunity
  - EN 61000-4-11 Voltage Dips and Sags
- ETSI
  - ETSI EN-300386-2 Telecommunication Network Equipment. Electromagnetic Compatibility Requirements

Compliance Statements for Environmental Requirements

Lithium Battery

Batteries in this product are not based on mercury, lead, or cadmium substances. The batteries used in this product are in compliance with EU Directives 91/157/EEC, 93/86/EEC, and 98/101/EEC. The product documentation includes instructional information on the proper method of reclamation and recycling.

Compliance Statements for EMC Requirements

- Canada on page 241
- European Community on page 243
- Japan on page 244
- Taiwan on page 244
- United States on page 244

Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. Industry Canada does not guarantee the equipment will operate to the users' satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

CAUTION: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

European Community

Declaration of Conformity

Juniper Networks, Inc.
1194 N. Mathilda Ave
Sunnyvale, CA. 94089 USA

declares that under our sole responsibility the product(s)

Internet Router
Model J4350/J6350

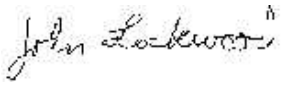
are in conformity with the provisions of the following EC Directives, including all amendments, and with national legislation implementing these directives:

Low Voltage Directive 73/23/EEC
EMC Directive 89/336/EEC

and that the following harmonized standards have been applied

EN 60950-1: 2001 + A11
EN 60825-1: 1994 +A1+A2

EN 300 386 V1.3.1:2001
EN 55024:1998
EN 55022:1998+A1+A2
EN 61000–3-2, EN 61000-3-3
EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5,
EN 61000-4-6, EN 61000-4-11



Place	Signature	Date
Sunnyvale, CA	John Lockwood	10/09/2006

Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

The preceding translates as follows:

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this product is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Taiwan

警告使用者
這是甲類的資訊產品，在居住的環境中使用時，
可能會造成射頻干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

United States

The Services Router has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Part 15 Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

FCC Part 68 Statement

This equipment complies with Part 68 of the Federal Communications Commission (FCC) rules. On the product is a label that contains the FCC registration number for this device. If requested, this information must be provided to the telephone company.

This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.

If this device causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. The telephone company may request that you disconnect the equipment until the problem is resolved. The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment or for repair or warranty information, please follow the applicable procedures explained in the “Technical Support” section of this manual.

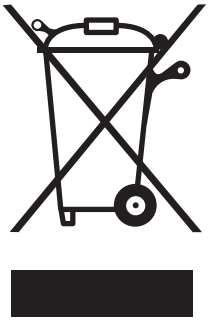
- FCC Registration Number—See label on product.
- Required Connector (USOC)—RJ-48C
- Service Order Code (SOC)—6.ON

Product Reclamation and Recycling Program

Juniper Networks is committed to environmentally responsible behavior. As part of this commitment, we continually work to comply with environmental standards such as the European Union's *Waste Electrical and Electronic Equipment* (WEEE) Directive and *Restriction of Hazardous Substances* (RoHS) Directive.

These directives and other similar regulations from countries outside the European Union regulate electronic waste management and the reduction or elimination of specific hazardous materials in electronic products. The WEEE Directive requires electrical and electronics manufacturers to provide mechanisms for the recycling and reuse of their products. The RoHS Directive restricts the use of certain substances that are commonly found in electronic products today. Restricted substances include heavy metals, including lead, and polybrominated materials. The RoHS Directive, with some exemptions, applies to all electrical and electronic equipment.

In accordance with Article 11(2) of Directive 2002/96/EC (WEEE), products put on the market after 13 August 2005 are marked with the following symbol or include it in their documentation: a crossed-out wheeled waste bin with a bar beneath.



Juniper Networks provides recycling support for our equipment worldwide to comply with the WEEE Directive. For recycling information, go to http://www.juniper.net/environmental, and indicate the type of Juniper Networks equipment that you wish to dispose of and the country where it is currently located, or contact your Juniper Networks account representative.

Products returned through our reclamation process are recycled, recovered, or disposed of in a responsible manner. Our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

Part 5

Index

Index

Symbols

[ ], in configuration statements xvii
{ }, in configuration statements xvii
( ), in syntax descriptions xvii
< >, in syntax descriptions xvii
| (pipe), in syntax descriptions xvii
* (red asterisk) 57
? command
  for CLI online help 63
  in configuration mode 61
  in operational mode 60
? icon (J-Web) 57
#, comments in configuration statements xvii
#, configuration mode command prompt 61
>, operational mode command prompt 60
4-Port Fast Ethernet ePIM 41
4-Port ISDN BRI S/T PIM
  description 42
  PIM ONLINE LED 44
4-Port ISDN BRI U PIM
  description 42
  PIM ONLINE LED 44

A

AC plug types 77
AC power
  connecting power 86
  cords *See* AC power cords
  dedicated AC power feed requirement 161
  electrical specifications 76
  grounding the router 87
  installing a J6350 power supply 161
  J4350 system 21
  J6350 system 21
  removing a J6350 power supply 160
  requirements 76
  safety guidelines 208
AC power cords
  electrical specifications 76
  physical requirements 76
  plug types 77
  replacing 159
accident, steps to take 215
ACTIVITY LED 41
ad0 *See* compact flash
addresses
  ge-0/0/0 for autoinstallation 97
  loopback 96
  management interface 97
ADSL PIM
  description 44
  PIM ONLINE LED 45
ADSL ports
  description 44
  LED states 45
  RJ-11 connector pinouts 199
agency approvals 240
air filter
  description 22
  location 171
  replacing 170
airflow
  description 23
  space requirement 71
ALARM LED
  description 18
  indications 172
alarms
  conditions, in chassis components 172
  LED 18
alternative boot media *See* boot devices; USB
altitude requirement 73
Annex A; Annex B *See* ADSL; SHDSL
antistatic mat 205
approvals, agency 240
asymmetric digital subscriber line *See* ADSL
AT modem command 103, 105
AT&D1 modem command 104
AT&K0 modem command 104
AT&W modem command 104
ATDT modem command 105
ATS0 = 1 modem command 104
autoinstallation
  automatic configuration process 127
  CLI configuration editor 128
  default configuration file 127
  description 97
  establishing 125

host-specific configuration file 127
interfaces..... 126
IP address procurement process..... 126
J-Web configuration editor 128
overview 126
protocols for procuring an IP address 126
requirements..... 127
status 130
TFTP server 126
verifying..... 129
automatic configuration *See* autoinstallation
AUX port 20
auxiliary console port.....20

B

backup router 96
defining (configuration editor) 111
basic connectivity
CLI configuration editor 108
establishing 93
J-Web configuration editor 108
Quick Configuration 105
requirements.....98
sample configuration 113
secure Web access.....115
verifying.....113
battery
environmental compliance..... 241
handling..... 232
lithium..... 241
BGP route reflectors license 132
blank panel
for PIM slots.....29
for power supply (J6350) 159
blinking
Fast Ethernet port ACTIVITY LED state 41
Fast Ethernet port link activity LED state.....42
Gigabit Ethernet port TX/RX LED state 19, 33
ISDN BRI ONLINE LED state 44
POWER LED state 17
STATUS (router) LED state 18
boot devices.....15
boot process, backup router for.....96
boot sequence 15
BOOTP, for autoinstallation..... 129
Border Gateway Protocol (BGP) route reflectors license 132
bottom pane 54
braces, in configuration statements..... xvii
brackets
angle, in syntax descriptions..... xvii
square, in configuration statements xvii
browser interface *See* J-Web interface
BTUs per hour.....73
built-in Ethernet ports *See* Gigabit Ethernet ports
buttons
power 17
RESET CONFIG 19

C

cables
AC power *See* AC power cords
ADSL RJ-11 pinouts 199
arranging for safety..... 146
connecting to network media.....85
console port, connecting 101, 104
console port, DB-9 connector pinouts 196
console port, replacing 144
console port, RJ-45 connector pinouts..... 195
DC cables *See* DC power cables
disconnecting PIM cables 148
E1 RJ-48 pinouts..... 196
Ethernet rollover, connecting 101, 104
Ethernet rollover, replacing..... 144
Ethernet, connecting 100
Fast Ethernet RJ-45 connector pinouts 194
Gigabit Ethernet RJ-45 connector pinouts 195
grounding 86
ISDN RJ-45 pinouts 199
PIM, installing..... 148
PIM, removing 148
reducing radio frequency interference (RFI) 75
serial EIA-530A DCE pinouts..... 190
serial EIA-530A DTE pinouts 189
serial PIM specifications..... 185
serial RS-232 DCE pinouts 187
serial RS-232 DTE pinouts..... 186
serial RS-422/449 (EIA-449) DCE pinouts 188
serial RS-422/449 (EIA-449) DTE pinouts..... 187
serial V.35 DCE pinouts 192
serial V.35 DTE pinouts..... 191
serial X.21 DCE pinouts 193
serial X.21 DTE pinouts..... 193
SHDSL RJ-11 pinouts..... 199
T1 RJ-48 pinouts..... 196
Canada, compliance statement 241
case number, for JTAC 178
certificates *See* SSL certificates
channelized E1 PIM.....36
channelized E1 ports
description 36
LED states.....38
RJ-48 cable pinouts 196
channelized T1 PIM.....36
channelized T1 ports
description 36
LED states.....38
RJ-48 cable pinouts 196
chassis
alarm conditions and remedies..... 172

component serial number labels 175
dimensions 14
environmental tolerances 73
grounding 86
J4350 9
J6350 9
lifting guidelines 221
PIM slot numbers 17
rack requirements 72
weight 14
chassis software process 24
chassisd process 24
checklist, for site preparation 79
clear operation, RESET CONFIG button 19
clear-text access 98
clearance 71
CLI configuration editor
autoinstallation 128
basic settings 108
capabilities 50
initial configuration 108
secure access configuration 121
statement types 61
command completion
description 63
setting on and off 66
command hierarchy 58
command prompts
changing 66
configuration mode (#) 61
operational mode (>) 60
command-line interface *See* CLI configuration editor; JUNOS CLI
comments, in configuration statements xvii
committed configuration
J-Web configuration editor display 57
root password requirement 95
Common Criteria environments
management access affected 98
NTP requirement 96
password limitations 95
compact flash
description 15
inserting 153
location (horizontal) 151
location (vertical) 150
minor (yellow) alarm 172
removing 152
replacing 149
replacing, rotating fans warning 152
compliance
EMC requirements 241
general standards 240
lithium battery 232
product reclamation and recycling 246
components
packing for shipment 181
replacing 143
serial number label 175
troubleshooting 171
See also LEDs
configuration
autoinstallation of 125
clearing with RESET CONFIG button 19
factory, resetting with RESET CONFIG button 19
installation on multiple Services Routers 125
root password requirement 95
configuration editor *See* CLI configuration editor; J-Web configuration editor
configuration hierarchy, J-Web display 57
configuration mode 62
commands 61
prompt (#) 61
See also CLI configuration editor
connection
AC power 86
DC power 88
for management 93
network cables 85
to Services Router 99
connectivity
basic *See* basic connectivity
hardware 81
modem (remote) connection 103
regaining lost DHCP lease after initial configuration 106
through J-Web 99
through the CLI locally 101
through the CLI remotely 103
console port
adapter 101, 104
auxiliary console port 20
connecting through the CLI locally 101
connecting through the CLI remotely 103
DB-9 connector pinouts 196
description 20
replacing the cable 144
RJ-45 connector pinouts 195
settings for local CLI connection 102
settings for modem connection at router for remote CLI access 103
settings for modem connection for remote CLI access 105
container statements 61
conventions
notice icons xvi
text and syntax xvi
cooling system
airflow requirement 71
description 22

Copper Gigabit Ethernet ePIMs
link speeds and transmission modes supported ...32
overview ...31
cords *See* AC power cords; cables; DC power cables
Crypto Accelerator Module
description ...15
installing ...169
location ...167
removing ...167
curly braces, in configuration statements ...xvii
customer support ...xx
contacting JTAC ...xx
contacting JTAC for hardware return ...178
information required for hardware return ...178

D

da0 *See* USB
daemons *See* processes, software
data link switching (DLSw) license ...132
datasheets URL ...27
DB-9 connector pinouts ...196
DB-9 to DB-25 serial port adapter ...104
DC power
cables *See* DC power cables
connecting power ...88
dedicated DC power feed requirement ...166
electrical specifications ...76
grounding requirements and warning ...211
grounding the router ...88
installing a J6350 power supply ...165
J4350 system ...21
J6350 system ...21
power disconnection warning ...210
removing a J6350 power supply ...163
requirements ...76
safety guidelines (general) ...209
safety guidelines, power sources for redundant power supplies ...209
wiring sequence warning ...212
wiring terminations warning ...213
DC power cables
electrical specifications ...77
physical requirements ...77
replacing ...162
usage warning ...209
Declaration of Conformity ...243
default configuration file, for autoinstallation ...127
default gateway ...96
defining (Quick Configuration) ...107
deleting
all configurations with RESCUE CONFIG button ...19
licenses (CLI) ...136
licenses (J-Web) ...135
DHCP (Dynamic Host Configuration Protocol) ...97
DHCP server
after initial configuration ...97
before initial configuration ...97
regaining lost lease after initial configuration ...106
diagnosis
chassis ...172
hardware ...172
dial-up modem connection *See* modem connection to router console port
digital certificate *See* SSL certificates
digital subscriber line *See* ADSL; SHDSL
DIMMs (dual inline memory modules) *See* DRAM modules
DLSw license ...132
DNS (Domain Name System) ...96
DNS server
defining (configuration editor) ...110
defining (Quick Configuration) ...107
function ...96
documentation set
comments on ...xx
domain name ...95
defining (configuration editor) ...109
defining (Quick Configuration) ...106
See also DNS server
Domain Name System ...96
domain search
defining (configuration editor) ...111
defining (Quick Configuration) ...107
downloading
configuration, with autoinstallation ...127
licenses (J-Web) ...135
DRAM modules
installing ...157
location ...155
removing ...156
dry chemical fire extinguishers, prohibited ...74
DS1 ports *See* E1 ports; T1 ports
DS3 ports *See* E3 ports; T3 ports
DSL *See* ADSL; SHDSL
dual inline memory modules *See* DRAM modules
Dual-Port Channelized T1/E1 PIM ...36
Dual-Port E1 PIM ...35
Dual-Port E3 PIM ...38
Dual-Port Fast Ethernet PIM ...40
Dual-Port Serial PIM ...34
Dual-Port T1 PIM ...35
Dual-Port T3 PIM ...38

E

E1 ports
description ...35
See also channelized E1 ports
LED states ...36
RJ-48 cable pinouts ...196

E3 ports
BNC connector pinouts ... 198
description ... 38
LED states ... 39
earth ground *See* grounding
earthquakes
rack-mount requirements ... 73
seismic requirements ... 73
EIA-530A DCE cable pinouts ... 190
EIA-530A DTE cable pinouts ... 189
electrical specifications ... 76
electricity
safety warnings ... 206
wiring guidelines ... 75
electromagnetic compatibility (EMC) *See* EMC
electromagnetic interference (EMI) *See* See EMI
electronic equipment, recycling ... 246
electrostatic bag, for storing components ... 205
electrostatic discharge, preventing ... 205
EMC (electromagnetic compatibility)
compliance with requirements ... 241
preventing problems with ... 75
standards ... 240
EMI (electromagnetic interference)
compliance with requirements ... 241
standards ... 240
suppressing ... 75
encrypted access
through HTTPS ... 115
through SSH ... 98
through SSL ... 115
environment, CLI
displaying ... 65
setting ... 65
environmental requirements for operation ... 73
ePIMs
4-Port Fast Ethernet ... 41
Copper Gigabit Ethernet ... 31
SFP Gigabit Ethernet ... 31
slot locations ... 17
EPROM ... 15
ESD (electrostatic discharge), preventing ... 205
ESD wrist strap
verifying resistance, for safety ... 205
wearing during installation ... 10
Ethernet cable
connecting the Services Router to a management device ... 100
DB-9 connector pinouts ... 196
replacing ... 144
RJ-45 connector pinouts ... 195
Ethernet ports *See* Fast Ethernet ports, Gigabit Ethernet ports
Ethernet rollover cable
connecting the Services Router to a management device ... 101
connecting the Services Router to a modem ... 104
DB-9 connector pinouts ... 196
replacing ... 144
RJ-45 connector pinouts ... 195
European Union, compliance statement ... 243

F

factory configuration, resetting with RESCUE CONFIG button ... 19
failures
compact flash, USB for ... 20
PIM ... 172
Routing Engine fan ... 173
fans ... 22
See also air filter
Fast Ethernet cable
RJ-45 connector pinouts ... 194
Fast Ethernet ports
4-Port Fast Ethernet ePIM ... 41
ACTIVITY status ... 41
Dual-Port Fast Ethernet PIM ... 40
LED states ... 41–42
link activity ... 42
link status ... 42
LINK/ SPEED status ... 41
RJ-45 connector pinouts ... 194
FCC Part 15 compliance statement ... 245
FCC Part 68 compliance statement ... 245
feature licenses *See* licenses
feature overview ... 5
field-replaceable units, replacing ... 143
filter cover *See* air filter
filter, air *See* air filter
fire extinguishers
prohibited ... 74
required ... 74
fire safety requirements ... 73
fire suppression
equipment required ... 74
shutdown requirement ... 74
font conventions ... xvi
forwarding software process ... 24
FPC, PIM slot number in command displays ... 147, 149, 175
front panel ... 16
FRUs (field-replaceable units), replacing ... 143
fwdd process ... 24

G

G.SHDSL PIM
description ... 46
PIM ONLINE LED ... 47

G.SHDSL ports *See* SHDSL ports
gateway, default....96
ge-0/0/0
connecting through J-Web....99
defining address (configuration editor)....112
defining address (Quick Configuration)....107
for autoinstallation....97
management interface....97
Gigabit Ethernet ePIMs....31
Gigabit Ethernet ports
built-in....19
LED states....19, 33
PIM port (copper)....32
PIM port (optical)....33
port 0....97
RJ-45 connector pinouts....195
glossary
autoinstallation....125
basic connectivity....93
PIMs....27
secure Web access....115
graceful shutdown....90
graphical user interface *See* J-Web interface
grounding
cable....86
chassis....86
DC power requirements and warning....211
equipment warning....214
grounding lug
connecting....87, 89
specifications....86
group licenses....134
GUI *See* J-Web interface

H

HA (high availability) LED....19
hardware
alarm conditions and remedies....172
installation and connection....81
maintenance....143
PIM overview....27
product overview....3
reclamation and recycling....246
replacing components....143
returning....175
troubleshooting components....171
See also LEDs
hardware features
components....13
front panel....16
PIMs....27
product overview....3
Hayes-compatible modem *See* modem connection to router console port
hazardous materials, reclamation and recycling....246
help
CLI command....64
J-Web interface....57
JUNOS CLI....63
help apropos command....64
help icon (?)....57
help reference command....64
help topic command....64
high availability (HA) LED....19
high-speed interfaces *See* ePIMs
high-speed slots for ePIMs, location....17
host-specific configuration file, for autoinstallation....127
hostname....95
defining (configuration editor)....109
defining (Quick Configuration)....106
overview....95
See also DNS server
hostname.conf file, for autoinstallation....127–128
HTTP (Hypertext Transfer Protocol)
enabling Web access (configuration editor)....121
enabling Web access (Quick Configuration)....117
on built-in management interfaces....116
verifying configuration....122
HTTPS (Hypertext Transfer Protocol over SSL)
enabling secure access (configuration editor)....121
enabling secure access (Quick Configuration)....117
Quick Configuration....117
recommended for secure access....116
verifying secure access configuration....122
humidity requirement....73
Hyperterminal, for terminal emulation
local CLI connection....102
modem connection at router for remote CLI access....103
modem connection for remote CLI access....105
Hypertext Transfer Protocol *See* HTTP
Hypertext Transfer Protocol over SSL *See* HTTPS

I

IBM networking *See* DLSw
idle time, setting for a CLI session....66
ifd process....24
immunity standards....240
initial configuration requirements....98
injury, steps to take....215
installation
AC power supplies (J6350)....161
air filter....170
compact flash disk....149
console port cable....144
Crypto Accelerator Module....169
DC power supplies (J6350)....165
DRAM modules....157
initial....81
licenses (CLI)....136

licenses (J-Web) ... 134
PIM cables ... 148
PIMs ... 146
preparation ... 71
requirements ... 81
restricted access, J4350 and J6350 ... 22, 83
safety guidelines and warnings ... 221
site checklist ... 79
site guidelines ... 71
USB storage device ... 155
Integrated Services Digital Network *See* ISDN
interface software process ... 24
interfaces
J4350 overview ... 4
J4350 types supported ... 30
J6350 overview ... 5
J6350 types supported ... 30
Internet Explorer, modifying for worldwide version of JUNOS software ... 53
ISDN BRI ports
BRI S/T ... 42
BRI U ... 42
LED states ... 44
provisioning ... 79
RJ-45 connector pinouts ... 199
ISDN provisioning ... 79
See also ISDN BRI ports

J

J-Flow license ... 132
J-series
autoinstallation ... 125
establishing secure Web access ... 115
establishing software connectivity ... 93
feature summary ... 5
hardware ... 9
hardware replacement ... 143
hardware return ... 175
HTTPS Web access ... 115
installation and connection ... 81
JUNOS Internet software overview ... 23
licenses ... 131
models available ... 3
network cables and connectors ... 185
PIMs ... 27
release notes, URL ... xv
safety and compliance ... 201
site preparation ... 71
SSL access ... 115
user interfaces ... 49
J-Web configuration editor
autoinstallation ... 128
basic settings ... 108
configuration hierarchy display ... 57
initial configuration ... 108
interface comparison ... 50
secure access ... 121
J-Web interface
configuration editor *See* J-Web configuration editor
connecting ... 99
context-sensitive help ... 57, 63
help (?) icon ... 57
Internet Explorer, modifying for worldwide version of JUNOS software ... 53
managing licenses ... 133
overview ... 49
page layout ... 53
Quick Configuration *See* Quick Configuration
regaining lost DHCP lease after initial configuration ... 106
sessions ... 58
starting ... 53
windows, multiple, unpredictable results with ... 58
J-Web Quick Configuration *See* Quick Configuration
J4350
4-Port Fast Ethernet ePIM ... 41
4-Port ISDN BRI S/T PIM ... 42
4-Port ISDN BRI U PIM ... 42
ADSL PIM ... 44
boot devices ... 15
boot sequence ... 15
chassis ... 9
cooling system ... 22
Dual-Port Channelized T1/E1 PIM ... 36
Dual-Port E1 PIM ... 35
Dual-Port Fast Ethernet PIM ... 40
Dual-Port Serial PIM ... 34
Dual-Port T1 PIM ... 35
electrical specifications ... 76
fans ... 22
front panel ... 16
FRUs, replacing ... 143
G.SHDSL PIM ... 46
Gigabit Ethernet ePIM ... 31
hardware ... 9
hardware components ... 13
hardware, replacing ... 143
installation ... 83
interfaces supported ... 30
physical specifications ... 14
PIM overview ... 29
PIMs supported ... 30
ports supported ... 30
power system ... 21
restricted access installation ... 22, 83
Routing Engine ... 14
USB port ... 20
J6350
4-Port Fast Ethernete PIM ... 41

4-Port ISDN BRI S/T PIM....42
4-Port ISDN BRI U PIM....42
ADSL PIM....44
boot devices....15
boot sequence....15
chassis....9
cooling system....22
Dual-Port Channelized T1/E1 PIM....36
Dual-Port E1 PIM....35
Dual-Port Fast Ethernet PIM....40
Dual-Port Serial PIM....34
Dual-Port T1 PIM....35
E3 PIM....38
electrical specifications....76
fans....22
front panel....16
FRUs, replacing....143
G.SHDSL PIM....46
Gigabit Ethernete PIM....31
hardware....9
hardware components....13
hardware, replacing....143
installation....83
interfaces supported....30
physical specifications....14
PIM overview....29
PIMs supported....30
ports supported....30
power supplies *See* power supplies, J6350
restricted access installation....22, 83
Routing Engine....14
T3 PIM....38
USB port....20
Japan, compliance statement....244
JTAC (Juniper Networks Technical Assistance Center)
contacting....173
contacting for hardware return....178
information required for hardware return....178
Juniper Networks Technical Assistance Center *See* JTAC
JUNOS CLI
command completion....63
command hierarchy....58
command modes....50
command prompts *See* command prompts
connecting locally....101
connecting remotely....103
context-sensitive help....63
editing keystrokes....62
environment, changing....65
idle time....66
managing licenses....136
overview....50
screen length....66
screen width....67
starting....59
terminal type....67
working directory....66
JUNOS Internet software
autoinstallation....125
establishing connectivity....93
establishing secure Web access....115
Internet Explorer, modifying for worldwide version....53
licenses....132
overview....23
Packet Forwarding Engine....24
processes....24
release notes, URL....xv
Routing Engine....24
worldwide version, modifying Internet Explorer for....53
JUNOScope application....26
JUNOScript API
defining access (Quick Configuration)....108
enabling secure access....117
management access....98
verifying secure access configuration....122
JUNOScript over SSL....117

K

kernel....24
key sequences, editing, in CLI....62

L

labels, serial number....175
laptop *See* management device
lasers
beam warning....229
Class 1 product warning....227
open aperture warning....230
safety guidelines....227
lead in equipment, reclamation and recycling....246
leaf statements....61
LEDs
ACTIVITY status....41
ADSL PIM status....45
ADSL port status....45
ALARM....18
channelized E1 ports....38
channelized T1 ports....38
Class 1 product warning....228
E1 port status....36
E3 port status....39
Fast Ethernet port status....41–42
G.SHDSL PIM status....47
Gigabit Ethernet port status....19, 33
HA....19
ISDN PIM status....44
ISDN port status....44
J4350 power supply....21

J6350 power supply ... 21
LAN port status ... 19
LINK ... 19, 33
link activity ... 42
link status ... 42
LINK/ SPEED status ... 41
ONLINE status (ADSL PIM) ... 45
ONLINE status (G.SHDSL PIM) ... 47
ONLINE status (ISDN BRI PIMs) ... 44
POWER ... 17
safety warnings ... 227
serial port status ... 34
SHDSL port status ... 47
STATUS (router) ... 18
T1 port status ... 36
T3 port status ... 39
TX/RX ... 19, 33
license infringement
identifying any licenses needed ... 134
verifying license usage ... 138
verifying licenses installed ... 137
license keys
components ... 132
displaying (CLI) ... 139
displaying (J-Web) ... 135
status ... 134
version ... 134
licenses
adding (CLI) ... 136
adding (J-Web) ... 134
BGP route reflectors ... 132
deleting (CLI) ... 136
deleting (J-Web) ... 135
displaying (CLI) ... 137
displaying (J-Web) ... 134
displaying usage ... 138
DLSw ... 132
downloading (J-Web) ... 135
features requiring a license ... 5
group ... 134
infringement, preventing ... 133
See also license infringement
installed ... 134
J-Flow traffic analysis ... 132
JUNOS Internet software ... 132
key ... 132
See also license keys
managing (CLI) ... 136
managing (J-Web) ... 133
overview ... 131
preparation for ... 132
saving (CLI) ... 137
traffic analysis ... 132
verifying ... 137
Licenses page ... 133
lifting guidelines ... 221
lightening activity warning ... 235
link activity LED ... 42
LINK LED ... 19, 33
link status LED ... 42
LINK/ SPEED LED ... 41
lithium battery compliance ... 241
lo0.0 ... 96
local connection to the router console port ... 101
loopback address
defining (configuration editor) ... 112
defining (Quick Configuration) ... 107
overview ... 96
lug *See* grounding lug

M

maintenance
AC power cord, replacing ... 159
air filter ... 170
console port cable ... 144
Crypto Accelerator Module ... 167
DC power cable, replacing ... 162
DRAM modules ... 155
PIM cables ... 147
PIMs ... 144
power system ... 158
primary compact flash ... 149
tools and parts required ... 144
USB storage device ... 153
warnings ... 231
major (red) alarms
PIMs ... 172
Routing Engine ... 173
management access ... 97
management device
connecting through the CLI ... 102
connecting to J-Web ... 100–101
management interface address
after initial configuration ... 97
before initial configuration ... 97
defining (configuration editor) ... 112
defining (Quick Configuration) ... 107
during initial configuration ... 97
management interfaces ... 97
autoinstallation on ... 126
loopback ... 96
management ports ... 19
See also management interface address; management interfaces
management software process ... 24
manuals
comments on ... xx
memory *See* compact flash; DRAM modules; USB
mgd process ... 24
microkernel ... 24

middle pane....57
midplane....14
minor (yellow) alarms
alternative boot device....172
primary compact flash....172
Routing Engine....173
modem commands
at remote end....105
at router end....103
modem connection to router console port
configuring modem at router end....103
configuring modem at user end....104
connecting modem to router....104
overview....103
monoammonium phosphate....74
mounting brackets
rack installation....85
multiple routers
deploying *See* autoinstallation
safe rack order....83

N

network cable pinouts....185
Network Time Protocol (NTP) server *See* NTP server
network.conf file, default for autoinstallation....127–128
notice icons....xvi
NT1 device, provisioning information....79
NTP server
defining (configuration editor)....110
defining (Quick Configuration)....106
overview....95
requirement for Common Criteria environments....96

O

ONLINE LEDs
ADSL PIM status....45
channelized E1 ports....38
channelized T1 ports....38
G.SHDSL PIM status....47
ISDN BRI PIM status....44
openssl command....117
operating system *See* JUNOS Internet software
operational mode
commands....60
prompt (>)....60

P

packaging, recycling....246
Packet Forwarding Engine....24
microkernel....24
packing materials
packing a Services Router for shipment....180
packing components for shipment....181
saving....82
pages, layout in J-Web....53
parentheses, in syntax descriptions....xvii
password *See* root password
PC *See* management device
PCI Express slots for ePIMs, location....17
personnel warning....204
PIC *See* PIMs
PIM number, always 0....147, 149
PIMs (Physical Interface Modules)
4-Port Fast Ethernet....41
4-Port ISDN BRI....42
ADSL....44
cables and connectors....185
Dual-Port Channelized T1/E1 PIM....36
Dual-Port E1....35
Dual-Port Fast Ethernet....40
Dual-Port Serial....34
Dual-Port T1....35
E3....38
failure....172
field-replaceable PIMs....29
G.SHDSL....46
Gigabit Ethernet....31
installing....146
installing cables....148
LEDs *See* LEDs
major (red) alarm....172
midplane to Routing Engine....14
overview....27
PIM number, always 0....147, 149, 175
removing....145
replacing cables....147
serial number label....177
slot number, in command output (FPC)....147
slot numbering....17
T3....38
pinouts
ADSL RJ-11 connector....199
console port....195
DB-9 connector....196
EIA-530A DCE serial cable....190
EIA-530A DTE serial cable....189
Fast Ethernet connector....194
Gigabit Ethernet connector....195
ISDN RJ-45 connector....199
RJ-45 console connector....195
RJ-48 connector to DB-15 connector (crossover)....198
RJ-48 connector to DB-15 connector (straight)....197
RJ-48 connector to RJ-48 connector (crossover)....197
RJ-48 connector to RJ-48 connector (straight)....196
RS-232 DCE serial cable....187
RS-232 DTE serial cable....186
RS-422/449 (EIA-449) DCE serial cable....188
RS-422/449 (EIA-449) DTE serial cable....187
SHDSL RJ-11 connector....199

V.35 DCE serial cable 192
V.35 DTE serial cable 191
X.21 DCE serial cable 193
X.21 DTE serial cable 193
plug types, AC 77
ports
0 97
ADSL *See* ADSL ports
AUX 20
cables, PIM, installing 148
cables, WAN, removing 148
channelized *See* channelized E1 ports; channelized T1 ports
console 20
See also console port
DS1 *See* E1 ports; T1 ports
DS3 *See* E3 ports; T3 ports
E1 *See* E1 ports
E3 *See* E3 ports
G.SHDSL *See* SHDSL ports
interface naming 147, 149
ISDN *See* ISDN BRI ports
J4350 types supported 30
J4350 USB 20
J6350 types supported 30
J6350 USB 20
lo0.0 96
serial *See* serial ports
SHDSL *See* SHDSL ports
T1 *See* T1 ports
T3 *See* T3 ports
power
AC power *See* AC power
applying 90
button 17
connecting 86
DC power *See* DC power
grounding requirement 86
LED 17
power cables *See* DC power cables
power cords *See* AC power cords
power supplies *See* power supplies
power system *See* power system
removing 91
requirements 76
power button 17
power cables *See* DC power cables
power cords *See* AC power cords
POWER LED 17
power supplies, J4350
LED states 21
power supplies, J6350
blank panel required in empty slot 159
dedicated AC power feed requirement 161
dedicated DC power feed requirement 166
description 21
installing AC 161
installing DC 165
LED states 21
redundancy 21
removing AC 160
removing DC 163
serial number label 177
power system
connecting 87–88
fan 22
J4350 21
J6350 21
power supply LED 21
preparing for installation 71
processes, software
chassis process 24
forwarding process 24
interface process 24
management process 24
routing protocol process 24
product disposal 238
product overview 3
prompt *See* command prompts; restart-after-upgrade prompt
provisioning an ISDN line 79

Q

Quick Configuration
basic settings 105
capabilities 50
initial configuration 105
Secure Access page 118
secure Web access 117
Set Up page 55

R

rack installation
general requirements 72
lifting guidelines 221
mounting brackets 85
order of multiple routers 83
procedure 83
safety guidelines and warnings 222
securing rack to building 73
size requirements 72
support for front-mount rack 72
ventilation requirement 72
radio frequency interference (RFI), reducing 75
ramp angle requirement 226
RARP, for autoinstallation 129
read or write error, Routing Engine 173
reclamation and recycling 246
recycling Juniper Networks equipment 246
red alarms *See* major (red) alarms

red asterisk (*) 57
redundant J6350 power supplies
  description 21
  safety guidelines for power sources 209
regulatory compliance 201
release notes, URL xv
remote connection to router console port
  configuring modem at router end 103
  configuring modem at user end 104
  connecting modem to router 104
  overview 103
replacement
  AC power cord 159
  air filter 170
  console port cable 144
  Crypto Accelerator Module 167
  DC power cable 162
  DRAM modules 155
  PIM cables 147
  PIMs 144
  power system (J6350) 158
  primary compact flash 149
  tools and parts required 144
  USB storage device 153
request chassis pic fpc-slot command 148
request system license add command 136
request system license add terminal command 136
request system license delete command 136
request system license save command 137
required entry (J-Web) 57
rescue configuration, resetting with RESCUE CONFIG button 19
reset
  power button for restart 17
  RESET CONFIG button for factory configuration 19
RESET CONFIG button
  for factory configuration 19
  for rescue configuration 19
restart-after-upgrade prompt 66
Restriction of Hazardous Substances (RoHS) Directive, recycling equipment 246
Return Materials Authorization *See* RMA
returning hardware 175
  packing a Services Router for shipment 180
  packing components for shipment 181
  procedure 178
  tools and parts required 179
Reverse Address Resolution Protocol (RARP), for autoinstallation 129
RJ-45 connector pinouts
  console port 195
  Fast Ethernet port 194
  Gigabit Ethernet port 195
RJ-45 to DB-9 serial port adapter 101, 104
RJ-48 connector to DB-15 connector (crossover) pinouts 198
RJ-48 connector to DB-15 connector (straight) pinouts 197
RJ-48 connector to RJ-48 connector (crossover) pinouts 197
RJ-48 connector to RJ-48 connector (straight) pinouts 196
RMA (Return Materials Authorization) 175
  number 178
  packing a Services Router for shipment 180
  packing components for shipment 181
  procedure 178
  tools and parts required 179
RoHS (Restriction of Hazardous Substances) Directive, recycling equipment 246
root password
  at initial local connection (none) 102
  at initial remote connection (none) 105
  characteristics 95
  Common Criteria limitations 95
  defining (configuration editor) 110
  defining (Quick Configuration) 106
  required to commit a configuration 95
route reflectors, BGP, license 132
router *See* Services Router
router.conf file, for autoinstallation 127
Routing Engine
  fan 22
  fan failure 173
  J4350 functions and components 14
  J6350 functions and components 14
  kernel 24
  major (red) alarm 173
  midplane to PIMs 14
  minor (yellow) alarm 173
  read or write error 173
  software component 24
  too hot 173
  too warm 173
routing protocol software process 24
rpd process 24
RS-232 DCE cable pinouts 187
RS-232 DTE cable pinouts 186
RS-422/449 (EIA-449) DCE cable pinouts 188
RS-422/449 (EIA-449) DTE cable pinouts 187

S

S/T port *See* ISDN BRI ports
safety guidelines and warnings
  AC power 208
  battery handling 232
  DC power (general) 209
  DC power disconnection 210
  DC power wiring sequence warning 212

DC power wiring terminations warning 213
DC power, grounding requirements and warning 211
DC power, redundant power supplies 209
electrical 207
general 203
grounded equipment 214
in case of electrical accident 215
installation 221
jewelry removal 233
lasers and LEDs 227
levels 201
lightening activity 235
maintenance and operation 231
multiple power supplies 215
operating temperature 236
power disconnection 217
product disposal 238
rack-mounting 222
ramps 226
read installation instructions 221
telecommunications cord 219
TN power system 218
safety standards 240
fire safety 73
sample configuration
for basic connectivity 113
for secure access 123
for SSL certificates 122
saving licenses (CLI) 137
screen length, CLI, setting 66
screen width, CLI, setting 67
SDX application 26
secure access
CLI configuration editor 121
generating SSL certificates 117
HTTPS access (configuration editor) 121
HTTPS access (Quick Configuration) 117
HTTPS recommended 116
installing SSL certificates (configuration editor) 121
installing SSL certificates (Quick Configuration) 117
J-Web configuration editor 121
JUNOScript SSL access 117
overview 116
requirements 117
sample configuration 123
verifying secure access configuration 122
Secure Access page
description 118
field summary 120
Secure Sockets Layer *See* SSL
Serial Line Address Resolution Protocol (SLARP), for autoinstallation 129
serial number
chassis components, label 175
PIMs 177
power supply 177
serial ports 34
autoinstallation on 126
cables and connectors 185
EIA-530A DCE pinouts 190
EIA-530A DTE pinouts 189
LED states 34
RS-232 DCE pinouts 187
RS-232 DTE pinouts 186
RS-422/449 (EIA-449) DCE pinouts 188
RS-422/449 (EIA-449) DTE pinouts 187
V.35 DCE pinouts 192
V.35 DTE pinouts 191
X.21 DCE pinouts 193
X.21 DTE pinouts 193
service provider, contacting for ISDN provisioning 79
Services Router
autoinstallation 125
backup 96
clearance 71
connecting 99
establishing secure Web access 115
establishing software connectivity 93
grounding a DC-powered model 88
grounding an AC-powered model 87
hardware 9
hardware replacement 143
hardware return 175
HTTPS Web access 115
installation and connection 81
licenses 131
multiple, deploying *See* autoinstallation
network cables and connectors 185
operating environment 73
overview 3, 5
packing for shipment 180
PIM overview 27
powering on and off 90
preparation checklist 79
safety and compliance 201
site preparation 71
software 23
SSL access 115
unpacking 82
user interfaces 49
sessions, J-Web 58
set cli commands 65
Set Up page 55
field summary 106
setup
configuration editor 108
Quick Configuration 105
requirements 98

SFP Gigabit Ethernet ePIMs
overview 31
SFPs supported 33
SFPs (small form-factor pluggable transceivers), on Gigabit Ethernet ePIMs....33
SHDSL ports
description 46
LED states on a G.SHDSL PIM....47
RJ-11 connector pinouts 199
shipping carton
packing a Services Router for shipment 180
packing components for shipment 181
saving 82
show chassis alarms command 172
show chassis fpc pic-status command 147, 149
show chassis hardware command
locating component serial numbers 175
verifying Crypto Accelerator Module installation 170
show cli command 65
show system license command 137
explanation 138
show system license keys command 139
show system license usage command 138
explanation 138
show system storage command 154
shutdown
graceful....90
immediate 90
side pane....57
signaling limitations 75
site preparation
checklist....79
electrical wiring guidelines....75
fire safety 73
for rack installation 72
guidelines 71
operating environment....73
power requirements....76
size
J4350....14
J6350....14
requirements for rack installation 72
SLARP, for autoinstallation 129
slot numbers, PIM
chassis diagram....17
displayed as FPC number in command output.... 147, 149
small form-factor pluggable transceivers *See* SFP
SNMP (Simple Network Management Protocol), no Gigabit Ethernet support....32
software 23
features....23
licenses *See* licenses
See also JUNOS Internet software
specifications
AC electrical connection....76
AC power cords....76
DC electrical connection 77
DC power cables....77
electrical 76
environmental 73
grounding cable....86
grounding lug 86
J4350 hardware....14
J6350 hardware....14
serial PIM cables and connectors 185
SSH
defining (configuration editor) 109
defining access (Quick Configuration) 108
management access....98
SSL (Secure Sockets Layer)
enabling secure access (Quick Configuration)....117
management access....116
verifying SSL configuration.... 122
SSL 3.0 option, disabling on Internet Explorer for worldwide version of JUNOS software 53
SSL certificates
adding (configuration editor).... 122
adding (Quick Configuration) 120
generating....117
sample configuration 122
verifying SSL configuration.... 122
standards compliance 240
startup
J-Web interface....53
JUNOS CLI....59
Services Router 90
statements, configuration types....61
status
autoinstallation 130
license key 134
router....18
See also STATUS LEDs
STATUS LEDs
ADSL ports....45
channelized E1 ports 38
channelized T1 ports 38
E1 ports 36
E3 ports 39
ISDN ports 44
router status....18
serial ports 34
SHDSL ports 47
T1 ports 36
T3 ports 39
storage media
replacing the primary compact flash 149
replacing the USB storage device 153
support, technical *See* technical support

symmetric high-speed digital subscriber line
See SHDSL
syntax conventions xvi
system overview
hardware 9
software 23
system time
defining (Quick Configuration) 107
overview 95
synchronizing (configuration editor) 110
synchronizing (Quick Configuration) 106

T

T1 ports
description 35
See also channelized T1 ports
LED states 36
RJ-48 cable pinouts 196
T3 ports
BNC connector pinouts 198
description 38
LED states 39
Taiwan, compliance statement 244
task bar 57
technical support
contacting JTAC xx
contacting JTAC for hardware return 178
information required for hardware return 178
telecommunications line wire gauge 219
Telnet
defining access (Quick Configuration) 107
management access 97
temperature
required for operation 73
Routing Engine, too hot 173
Routing Engine, too warm 173
warning 236
temperature alarm, air filter replacement for 170
terminal type, setting 67
terminology
autoinstallation 125
basic connectivity 93
PIMs 27
secure Web access 115
TFTP, for autoinstallation 126
thermal output 73
time *See* system time
time zone 95
defining (configuration editor) 110
defining (Quick Configuration) 106
TN power system 218
tolerances, environmental 73
tools and equipment
for component replacement 144
for hardware return 179
top pane 57
traffic analysis license 132
Trivial File Transfer Protocol (TFTP), for
autoinstallation 126
troubleshooting a Services Router, hardware
components 171
See also LEDs
turning on a Services Router 90
TX/RX LED 19, 33
Type C fire extinguishers 74
types of configuration statements 61

U

U port *See* ISDN BRI ports
United States, compliance statements 244
universal serial bus *See* USB
unpacking the router 82
URLs
datasheets 27
PIM information and datasheets 27
release notes xv
return and repair policies 178
support 173
USB (universal serial bus)
J4350 USB port 20
J6350 USB port 20
storage device, installing 155
storage device, removing 154
storage device, replacing 153
user interfaces
feature comparison 50
J-Web graphical user interface (GUI) 26
See also J-Web interface
JUNOS command-line interface (CLI) 26
See also JUNOS CLI
JUNOScope application 26
overview 49
preparation 52
SDX application 26

V

V.35 DCE cable pinouts 192
V.35 DTE cable pinouts 191
ventilation requirement 71
verification
active licenses 137
autoinstallation 129
basic connectivity 113
license usage 138
licenses 137
secure access 122
version
license key 134

W

warnings
- battery handling ... 232
- DC power cables ... 209
- DC power disconnection ... 210
- DC power plant and chassis ground ... 78
- DC wiring sequence ... 212
- DC wiring terminations ... 213
- DC-powered J4350 and J6350 routers, restricted access installation only ... 75
- earthed mains socket (Norway and Sweden only) ... 215
- electrical ... 206
- ESD strap to prevent router damage ... 10
- follow lifting guidelines ... 83
- general ... 203
- grounded equipment ... 214
- installation ... 221
- jewelry removal ... 233
- laser and LED ... 227
- levels defined ... 201
- lightening activity ... 235
- maintenance and operational ... 231
- multiple power supply disconnection ... 215
- operating temperature ... 236
- personnel ... 204
- power disconnection ... 217
- product disposal ... 238
- rack-mounting requirements ... 222
- ramp angle ... 226
- read installation instructions ... 221
- restricted access location for DC-powered routers ... 22, 83
- rotating fans, compact flash replacement ... 152
- safe rack order for multiple routers ... 83
- telecommunications lines ... 219
- TN power system ... 218

Waste Electrical and Electronic Equipment (WEEE) Directive, recycling equipment ... 246
Web access, secure *See* secure access
Web browser, modifying Internet Explorer for worldwide version of JUNOS software ... 53
WEEE (Waste Electrical and Electronic Equipment) Directive, recycling equipment ... 246
weight
- J4350 ... 14
- J6350 ... 14
- rack-mount requirements ... 72

windows, J-Web, unpredictable results with multiple ... 58
wire gauge
- for grounding cables ... 86
- for telecommunications lines ... 219

wiring guidelines
- DC wiring sequence warning ... 212
- DC wiring terminations warning ... 213
- radio frequency interference (RFI) ... 75
- signaling limitations ... 75
- suppressing electromagnetic interference (EMI) ... 75

working directory, setting ... 66

X

X.21 DCE cable pinouts ... 193
X.21 DTE cable pinouts ... 193

Y

yellow alarm *See* minor (yellow) alarms