## J2300, J4300, and J6300 Services Router

# Getting Started Guide

*Release 8.5*

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

Part Number: 530-021975-01, Revision 1

*J2300, J4300, and J6300 Services Router Getting Started Guide*
Release 8.5
Copyright © 2007, 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., and Alan Twhigg
Editing: Taffy Everts and Stella Hackell
Illustration: Faith Bradford Brown and Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
12 October 2007—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

# Table of Contents

## Part 5 Index

# About This Guide

This preface provides the following guidelines for using the *J2300, J4300, and J6300 Services Router Getting Started Guide*:



## Objectives

This guide contains an overview, basic instructions, and specifications for J2300, J4300, and J6300 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.

J-series Services Router operations are controlled by the JUNOS software. You direct the JUNOS software through either a Web browser or a command-line interface (CLI).

**NOTE:** This guide documents Release 8.5 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.

## 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 1 on page xvi defines the notice icons used in this guide.

**Table 1: Notice Icons**

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

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

**Table 2: Text and Syntax Conventions**

| Convention | Description | Examples |
|---|---|---|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the **configure** command:<br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host> show chassis alarms`<br>`No alarms currently active` |
| *Italic text like this* | ■ Introduces important new terms.<br>■ Identifies book names.<br>■ Identifies RFC and Internet draft titles. | ■ A policy *term* is a named structure that defines match conditions and actions.<br>■ *JUNOS System Basics Configuration Guide*<br>■ RFC 1997, *BGP Communities Attribute* |

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

| Convention | Description | Examples |
|---|---|---|
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br>[edit]<br>root@# **set system domain-name** *domain-name* |
| Plain text like this | Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components. | ■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.<br>■ 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<br>(*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]<br>routing-options {<br>static {<br>route default {<br>nexthop *address*;<br>retain;<br>}<br>}<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| **J-Web GUI Conventions** | | |
| **Bold text like this** | Represents J-Web graphical user interface (GUI) items you click or select. | ■ In the Logical Interfaces box, select **All Interfaces**.<br>■ 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 3 on page xviii.

**Table 3: 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"<br>"Establishing Basic Connectivity" | ■ *JUNOS CLI User Guide*<br>■ *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*<br>■ *JUNOS System Basics Configuration Guide* |
| "Interfaces Overview"<br>"Configuring DS1, DS3, Ethernet, and Serial Interfaces"<br>"Configuring Channelized T1/E1/ISDN PRI Interfaces"<br>"Configuring Digital Subscriber Line Interfaces<br>"Configuring Point-to-Point Protocol over Ethernet"<br>"Configuring ISDN"<br>"Configuring VoIP" | ■ *JUNOS Network Interfaces Configuration Guide*<br>■ *JUNOS Interfaces Command Reference* |
| "Configuring Link Services Interfaces" | ■ *JUNOS Services Interfaces Configuration Guide*<br>■ *JUNOS System Basics and Services Command Reference* |
| "Routing Overview"<br>"Configuring Static Routes"<br>"Configuring a RIP Network"<br>"Configuring an OSPF Network"<br>"Configuring the IS-IS Protocol"<br>"Configuring BGP Sessions" | ■ *JUNOS Routing Protocols Configuration Guide*<br>■ *JUNOS Routing Protocols and Policies Command Reference* |
| **J-series Services Router Advanced WAN Access Configuration Guide** | |
| "Multiprotocol Label Switching Overview"<br>"Configuring Signaling Protocols for Traffic Engineering"<br>"Configuring Virtual Private Networks"<br>"Configuring CLNS VPNs" | ■ *JUNOS MPLS Applications Configuration Guide*<br>■ *JUNOS Routing Protocols and Policies Command Reference*<br>■ *JUNOS VPNs Configuration Guide* |

**Table 3: J-series Guides and Related JUNOS Software Publications** *(continued)*

| Chapter in a J-series Guide | Corresponding JUNOS Software Manual |
|---|---|
| "Configuring IPSec for Secure Packet Exchange" | ■ *JUNOS System Basics Configuration Guide*<br>■ *JUNOS Services Interfaces Configuration Guide*<br>■ *JUNOS System Basics and Services Command Reference* |
| "Multicast Overview"<br>"Configuring a Multicast Network" | ■ *JUNOS Multicast Protocols Configuration Guide*<br>■ *JUNOS Routing Protocols and Policies Command Reference* |
| "Configuring Data Link Switching" | ■ *JUNOS Services Interfaces Configuration Guide*<br>■ *JUNOS System Basics and Services Command Reference* |
| "Policy Framework Overview"<br>"Configuring Routing Policies" | ■ *JUNOS Policy Framework Configuration Guide*<br>■ *JUNOS Routing Protocols and Policies Command Reference* |
| "Configuring NAT"<br>"Configuring Stateful Firewall Filters and NAT"<br>"Configuring Stateless Firewall Filters" | ■ *JUNOS Network Interfaces Configuration Guide*<br>■ *JUNOS Policy Framework Configuration Guide*<br>■ *JUNOS Services Interfaces Configuration Guide*<br>■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS*<br>■ *JUNOS System Basics and Services Command Reference*<br>■ *JUNOS Routing Protocols and Policies Command Reference* |
| "Class-of-Service Overview"<br>"Configuring Class of Service" | ■ *JUNOS Class of Service Configuration Guide*<br>■ *JUNOS System Basics and Services Command Reference* |
| **J-series Services Router Administration Guide** | |
| "Managing User Authentication and Access" | ■ *JUNOS System Basics Configuration Guide*<br>■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS* |
| "Setting Up USB Modems for Remote Management"<br>"Configuring SNMP for Network Management" | *JUNOS Network Management Configuration Guide* |
| "Configuring the Router as a DHCP Server"<br>"Configuring Autoinstallation" | *JUNOS System Basics Configuration Guide* |
| "Automating Network Operations and Troubleshooting" | *JUNOS Configuration and Diagnostic Automation Guide* |
| "Monitoring the Router and Routing Operations" | ■ *JUNOS System Basics and Services Command Reference*<br>■ *JUNOS Interfaces Command Reference*<br>■ *JUNOS Routing Protocols and Policies Command Reference* |
| "Monitoring Events and Managing System Log Files" | ■ *JUNOS System Log Messages Reference*<br>■ *Secure Configuration Guide for Common Criteria and JUNOS-FIPS* |

**Table 3: J-series Guides and Related JUNOS Software Publications** *(continued)*

| Chapter in a J-series Guide | Corresponding JUNOS Software Manual |
|---|---|
| "Configuring and Monitoring Alarms" | *JUNOS System Basics Configuration Guide* |
| "Performing Software Upgrades and Reboots" | *JUNOS Software Installation and Upgrade Guide* |
| "Using Services Router Diagnostic Tools" | ■ *JUNOS System Basics and Services Command Reference*<br>■ *JUNOS Interfaces Command Reference*<br>■ *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

Chapter 1

# Overview of J2300, J4300, and J6300 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 interface—A Web-based graphical interface that allows you to operate a router without commands. The J-Web interface provides access to all JUNOS functionality and features. Quick Configuration wizards simplify basic configuration and minimize the risk of operator error.
- JUNOS command-line interface—A Juniper Networks command shell that runs on top of a UNIX-based operating system kernel. The CLI is a straightforward command interface. On a single line, you type commands that 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 61. For more information, see the *J-Web Interface User Guide* and the *JUNOS CLI User Guide*.

This chapter contains the following topics:

## J2300 Services Router Overview

The J2300 Services Router is primarily designed for remote or branch offices.

The J2300 Services Router features a smaller chassis (1 U) with a nonredundant AC or DC power supply, 256 MB to 1 GB of memory, a Universal Serial Bus (USB) port for external storage, and installation options for desktop installation, wall mounting, or rack mounting. Each J2300 Services Router has two Fast Ethernet LAN interfaces and two additional physical interfaces that depend on the chassis type. Available chassis types include the following:

- Dual-Port E1 chassis
- Dual-Port E1 with ISDN BRI S/T chassis
- Dual-Port Serial chassis
- Dual-Port Serial with ISDN BRI S/T or U chassis
- Dual-Port T1 chassis
- Dual-Port T1 with ISDN BRI U chassis
- Dual-Port G.SHDSL chassis
- Dual-Port G.SHDSL with ISDN BRI S/T chassis

## J4300 Services Router Overview

The J4300 Services Router is primarily designed for regional or branch offices.

The J4300 Services Router has a larger chassis (2 U) with a nonredundant AC or DC power supply, 256 MB to 1 GB of memory, and a Universal Serial Bus (USB) port for external storage. Each J4300 Services Router has two fixed Fast Ethernet LAN interfaces, and six open slots in which you can install the following Physical Interface Modules (PIMs):

- ADSL 2/2+ Annex A PIM (1 port)
- ADSL 2/2+ Annex B PIM (1 port)
- Channelized T1/E1 PIM
- Dual-Port Channelized T1/E1
- Dual-Port E1 PIM
- Dual-Port Fast Ethernet PIM
- G.SHDSL PIM (2 ports)
- 4-port ISDN BRI S/T or U PIM
- Dual-Port Serial PIM
- Dual-Port T1 PIM

## J6300 Services Router Overview

The J6300 Services Router is designed primarily for large branches or regional offices.

The J6300 Services Router has a larger chassis (2 U) with an optional redundant AC or DC power supply, 256 MB to 1 GB of memory, and a Universal Serial Bus (USB) port for external storage. Each J6300 Services Router has two fixed Fast Ethernet LAN interfaces, and six open slots in which you can install the following Physical Interface Modules (PIMs):

- ADSL 2/2 + Annex A PIM (1 port)
- ADSL 2/2 + Annex B PIM (1 port)
- Channelized T1/E1 PIM
- DS3 (T3) PIM (1 port)
- Dual-Port E1 PIM
- E3 PIM (1 port)
- Dual-Port Fast Ethernet PIM
- 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 4 on page 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 4: Summary of J-series Features and License Requirements**

| Feature Category | J-series Feature | Separate License |
|---|---|---|
| **Internet Protocols** | IPv4 | |
| | IPv6 routing and forwarding | |

**Table 4: Summary of J-series Features and License Requirements** *(continued)*

| Feature Category | J-series Feature | Separate License |
|---|---|---|
| **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):<br>■ End system-to-Intermediate system (ES-IS) protocol<br>■ IS-IS extensions<br>■ BGP extensions<br>■ Static routes | |
| | Multiprotocol Label Switching (MPLS):<br>■ Layer 2 and Layer 3 virtual private networks (VPNs)<br>■ VPN routing and forwarding (VRF) table labels<br>■ Traffic engineering protocols:<br>  ■ Label Distribution Protocol (LDP)<br>  ■ Resource Reservation Protocol (RSVP) | |
| | Multicast:<br>■ Internet Group Management Protocol version 3 (IGMPv3)<br>■ Protocol Independent Multicast (PIM)<br>■ Distance Vector Multicast Routing Protocol (DVMRP)<br>■ Single-source multicast | |
| **IP Address Management** | Static addresses | |
| | Dynamic Host Configuration Protocol (DHCP) | |

**Table 4: Summary of J-series Features and License Requirements** *(continued)*

| Feature Category | J-series Feature | Separate License |
|---|---|---|
| **Encapsulation** | Ethernet:<br>■ Media access control (MAC) encapsulation<br>■ 802.1p tagging<br>■ Point-to-Point Protocol over Ethernet (PPPoE)<br>■ Asynchronous Transfer Mode (ATM) for asymmetric digital subscriber line (ADSL) or symmetric high-speed digital subscriber line (SHDSL)<br>■ Circuit cross-connect (CCC)<br>■ 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 | |

**Table 4: Summary of J-series Features and License Requirements** *(continued)*

| Feature Category | J-series Feature | Separate License |
|---|---|---|
| **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) | |
| **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, SSH, or J-Web CLI terminal | |
| | 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 | |

**Table 4: Summary of J-series Features and License Requirements** *(continued)*

| Feature Category | J-series Feature | Separate License |
|---|---|---|
| **Administration** | Supports the following external administrator databases:<br>■ RADIUS<br>■ 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:<br>■ Commit scripts<br>■ Operation scripts<br>■ Event policies | |

Chapter 2

# System Overview

J-series Services Routers are available in several models.

This chapter contains the following topics:



## J2300 Services Router Hardware Features

This section contains the following topics:



### *J2300 Chassis*

The J2300 Services Router chassis is a rigid sheet metal structure that houses all the other router components (see Figure 1 on page 12, Figure 2 on page 12, and Figure 4 on page 13). The chassis can be installed in many types of racks or cabinets, on a wall, or on a desk. For information about acceptable rack types, see "Rack Requirements" on page 80.

In addition to the features described in subsequent sections, the chassis includes the following features (see Figure 1 on page 12 through Figure 3 on page 13):

- One pair of metal brackets that can be attached to the side of the chassis. You can use the brackets for mounting the chassis in a rack or cabinet or on a wall.
- One electrostatic discharge (ESD) point, a PEM nut at the rear 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 terminal on the rear of the chassis is provided to connect the router to ground (see Figure 2 on page 12). 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 191.

**Figure 1: Front of J2300 Chassis**

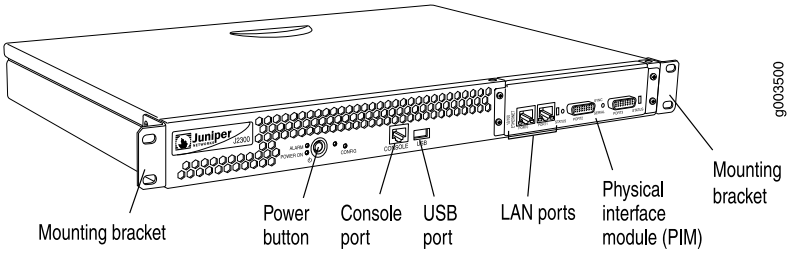



**Figure 2: Rear of J2300 AC-Powered Chassis**

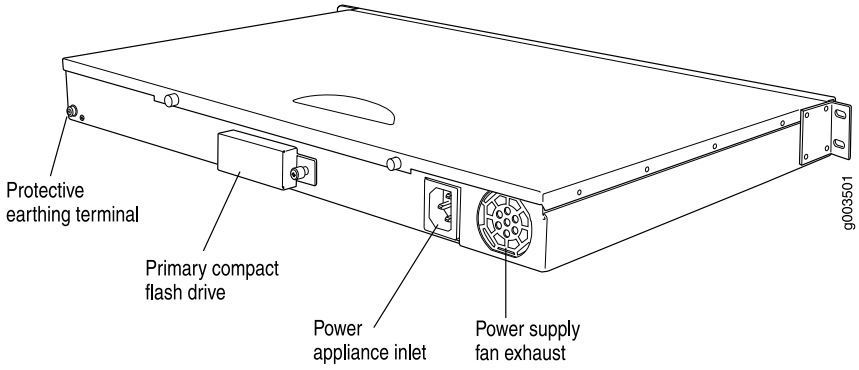


**Figure 3: Rear of J2300 DC-Powered Chassis**

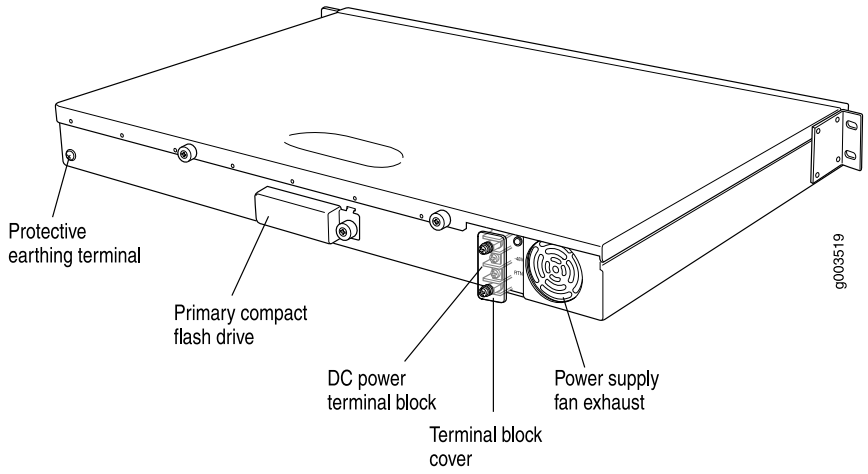



**Figure 4: J2300 Hardware Components**

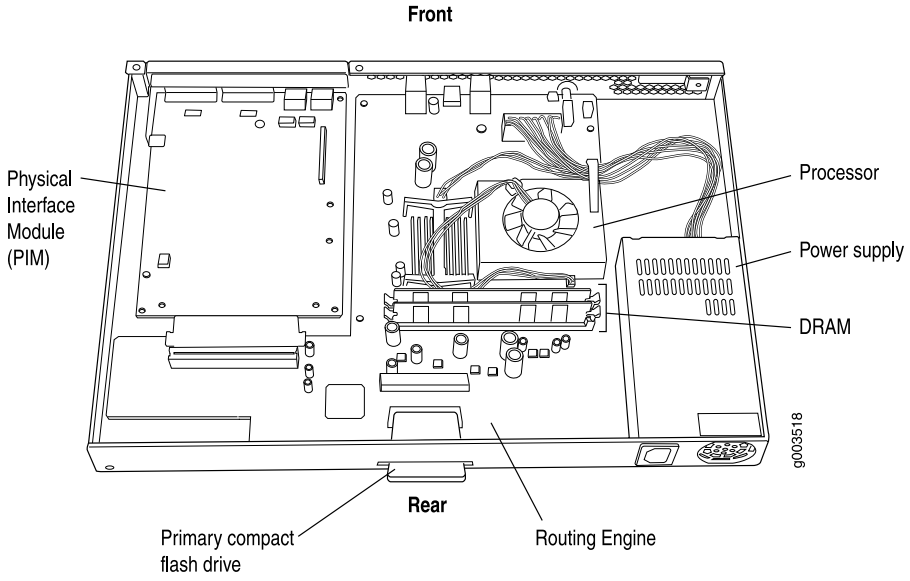



Table 5 on page 13 summarizes the physical specifications for the J2300 router chassis.

**Table 5: J2300 Physical Specifications**

| Description | Value |
|---|---|
| Chassis dimensions | ■ 1.75 in. (4.4 cm) high<br>■ 17.25 in. (43.8 cm) wide—19 in. (48.3 cm) wide with mounting brackets attached<br>■ 12.37 in. (31.4 cm) deep—plus 0.5 in. (1.27 cm) of hardware that protrudes from the chassis front |

**Table 5: J2300 Physical Specifications** *(continued)*

| Description | Value |
|---|---|
| Router weight | 12 lb (5.4 kg) |

## *J2300 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.
- Compact flash drive—Provides primary storage for software images, configuration files, and microcode. The primary compact flash drive is accessible from the rear of the router. For information about replacing the primary compact flash drive, see “Removing and Installing the Primary Compact Flash Disk” on page 148.

### J2300 Boot Devices

The J2300 Services Router can boot from two devices:

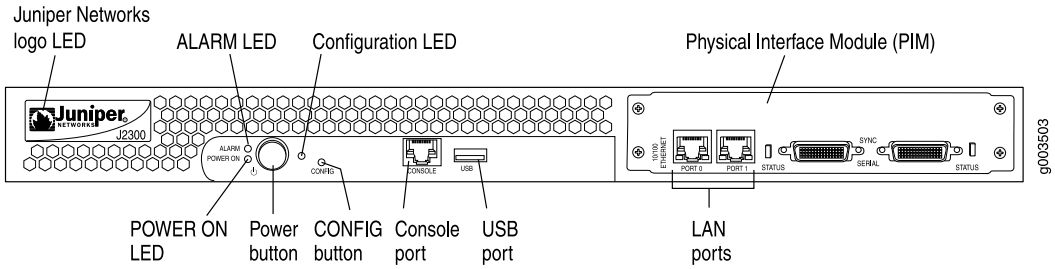
- Primary compact flash disk
- USB storage device

Normally, the Services Router boots from the primary compact flash disk. If the compact flash disk fails, the router attempts to boot from the removable USB storage device, if present, which is the alternate boot device.

## J2300 Front Panel

The front panel of the Services Router (Figure 5 on page 15) allows you to view router status LEDs, access the console port, and perform simple control functions.

**Figure 5: Front Panel of J2300 Services Router**




For information about the components of the front panel, see the following sections:

- Juniper Networks Logo LED on page 15
- ALARM LED on page 16
- Power Button and POWER LED on page 16
- CONFIG Button on page 17
- Console Port on page 17
- J2300 USB Port on page 18

### Juniper Networks Logo LED

The Juniper Networks logo LED is located on the top-left corner on the front panel (see Figure 5 on page 15). Table 6 on page 15 describes the blue Juniper Networks logo LED.

**Table 6: Juniper Networks Logo LED**

| Color | State | Description |
|---|---|---|
| Blue | Off | Router is unplugged, powered off, or malfunctioning. |
| | On steadily | Router is functioning normally. |
| | Blinking | ■ Router is booting and not yet forwarding traffic.<br>Or<br>■ Router is operating but unable to forward traffic because of a problem.<br><br>For a list of alarms that can occur on the router, see "Chassis Alarm Conditions" on page 165. |

### ALARM LED

The ALARM LED is located to the left of the power button on the front panel (see Figure 5 on page 15). The yellow (amber) LED lights to indicate a critical condition that can result in a system shutdown or a less severe condition that requires monitoring or maintenance. When the condition is corrected, the light turns off.

**NOTE:** The ALARM LED on the Services Router lights yellow whether the alarm condition is major (red) or minor (yellow).

To deactivate alarms, you must clear the condition that caused the alarm. For a list of alarms that can occur on the router, see "Chassis Alarm Conditions" on page 165.

### Power Button and POWER LED

The power button is located on the left side of the front panel (see Figure 5 on page 15). 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 left of the power button on the front panel. Table 7 on page 16 describes the POWER LED.

**Table 7: POWER LED**

| Color | State | Description |
|---|---|---|
| Green | Off | Router is unplugged, or is powered off and in standby mode. |
| | On steadily | Router is powered on and is either booting or functioning normally. |
| | Blinking | Power button has been pressed and quickly released, and the router is gracefully shutting down. |

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*.

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.

### CONFIG Button

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

The CONFIG button performs two recovery operations:

- Rescue—Press and release the CONFIG button to load and commit the rescue configuration, if you have set it. To set the rescue configuration, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.
- Clear—Press and hold the CONFIG button for 15 seconds or more, until the configuration LED blinks red to indicate the clear operation is in progress. The clear operation deletes *all* configurations on the router (including the rescue configuration and backup configurations) and loads and commits the factory configuration.

**CAUTION:** Pressing and holding the CONFIG button for 15 seconds or more deletes *all* configurations on the router and loads and commits the factory configuration.

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

Table 8 on page 17 describes the configuration LED.

**Table 8: Configuration LED**

| Color | State | Description |
|---|---|---|
| Green | Blinking | Rescue configuration is being loaded. |
| | On steadily | Rescue or factory configuration is loaded and committed. |
| Red | Blinking | ■ Current committed configuration and all previous versions are being deleted.<br>■ Factory configuration is being loaded. |
| | On steadily | Operation to return the router to the rescue or factory configuration failed. |

### Console Port

You can use the console port on the chassis front panel to connect to the Routing Engine through an RJ-45 serial cable. From the chassis 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 chassis console port, see the *J-series Services Router Administration Guide*.

For pinout information, see "Chassis Console Port Pinouts" on page 185.

### J2300 USB Port

The slot labeled USB on the front panel of the router (see Figure 5 on page 15) accepts 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 the 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.

## J2300 Physical Interface Module (PIM)

The PIMs in J2300 Services Routers are fixed and not interchangeable, with different chassis types providing different PIMs. The PIMs provide the physical connection to various network media types. J2300 Services Routers are available with different types of chassis. Each chassis type contains two Fast Ethernet LAN ports, one set of WAN ports, and additional fixed PIMs of different types. For more information, see "J2300 Chassis with Fixed PIMs" on page 38.

For pinouts of PIM cable connectors, see "Network Cable Specifications and Connector Pinouts" on page 175.

## J2300 LAN Ports

The J2300 Services Routers include two fixed 10/100Base-TX Fast Ethernet ports. The LAN ports receive incoming packets from the network and transmit outgoing packets to the network. Each port 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.

The LAN ports are located on the front panel of the router (see Figure 5 on page 15) and are configured like the ports on a Physical Interface Module (PIM). The LAN ports are not field-replaceable. The ports, labeled PORT 0 and PORT 1, correspond to fe-0/0/0 and fe-0/0/1, respectively, for configuration.

For pinouts of Fast Ethernet cable connectors, see "Network Cable Specifications and Connector Pinouts" on page 175.

Each port has two LEDs located on each side of the bottom of the port. Table 9 on page 19 describes the LAN port LEDs.

**Table 9: LEDs for Fast Ethernet LAN Ports**

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

## *J2300 Power System*

The J2300 Services Router uses either AC or DC power. The autosensing power supply (see Figure 2 on page 12 or Figure 3 on page 13) 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. An 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) requiring a dedicated 15 A (–48 VDC) circuit breaker.

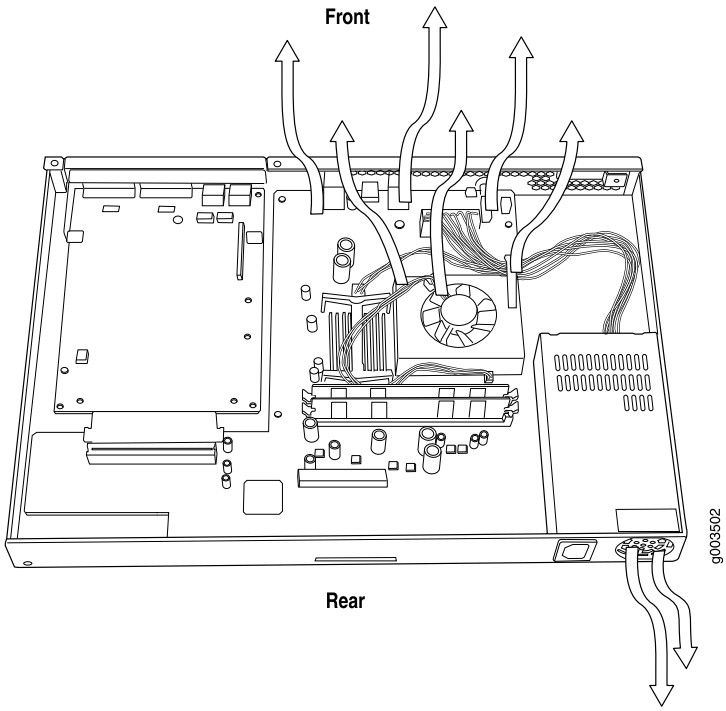
For information about site power preparations, see "Power Guidelines, Requirements, and Specifications" on page 83. For information about connecting the router to power and ground, see "Connecting Power" on page 96.

## *J2300 Cooling System*

The cooling system includes a fan on the rear of the Routing Engine's processor and a fan on the power supply.

The airflow produced by these fans keeps router components within the acceptable temperature range (see Figure 6 on page 20). The speed of the fan at the rear of the processor is adjusted automatically according to current temperature.

**Figure 6: Airflow Through the J2300 Chassis**




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.

## J4300 and J6300 Services Router Hardware Features

This section contains the following topics:



### *J4300 and J6300 Chassis*

The J4300 and J6300 Services Router chassis is a rigid sheet metal structure that houses all the other router components (see Figure 7 on page 21 through

Figure 12 on page 24). The chassis can be installed in many types of racks or cabinets. For information about acceptable rack types, see "Rack Requirements" on page 80.

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

- One pair of metal brackets attached to the side of the chassis. You can use the brackets for mounting the chassis in a rack or cabinet.
- One protective earthing terminal, a PEM nut 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 terminal on the rear of the chassis is provided to connect the router to ground (see Figure 8 on page 22). 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 191.

---

**Figure 7: Front of J4300 and J6300 Chassis**

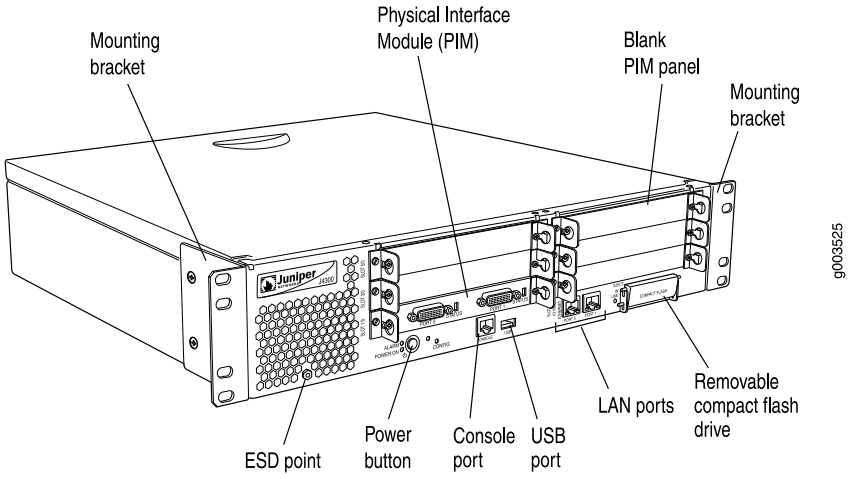


**Figure 8: Rear of AC-Powered J4300 Chassis**

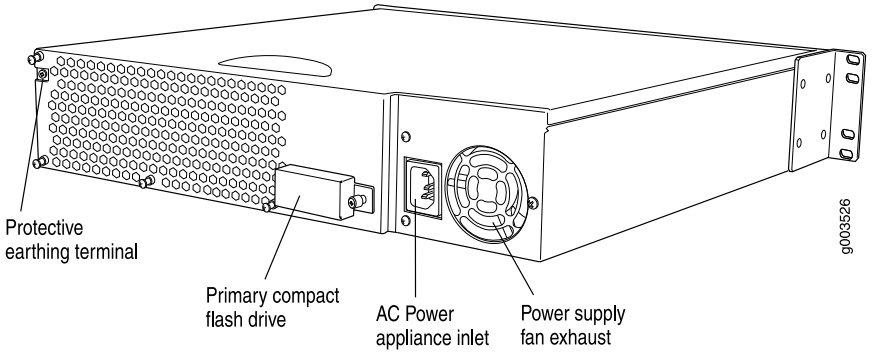



**Figure 9: Rear of DC-Powered J4300 Chassis**

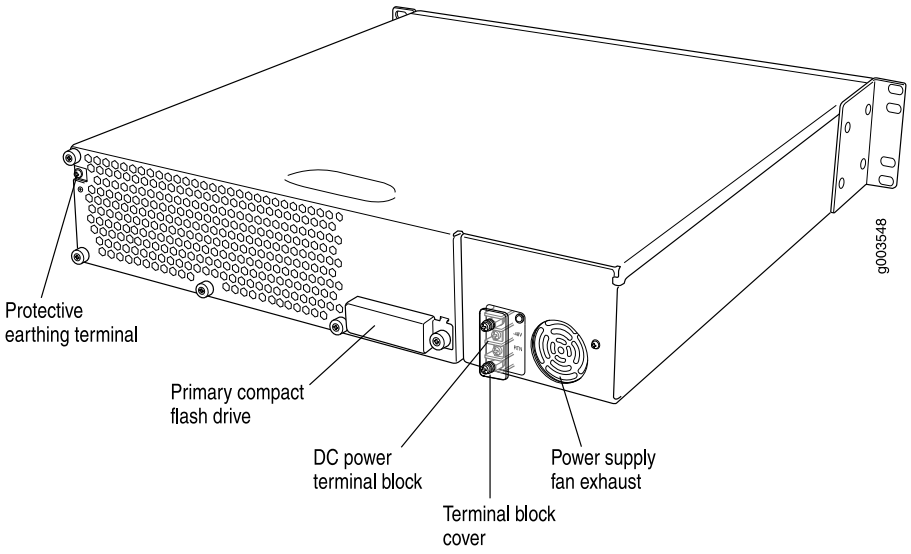



**Figure 10: Rear of AC-Powered J6300 Chassis**

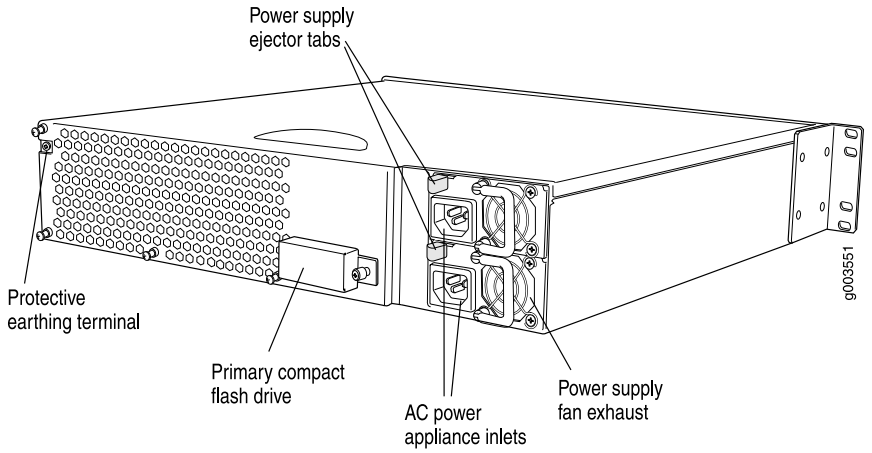


**Figure 11: Rear of DC-Powered J6300 Chassis**

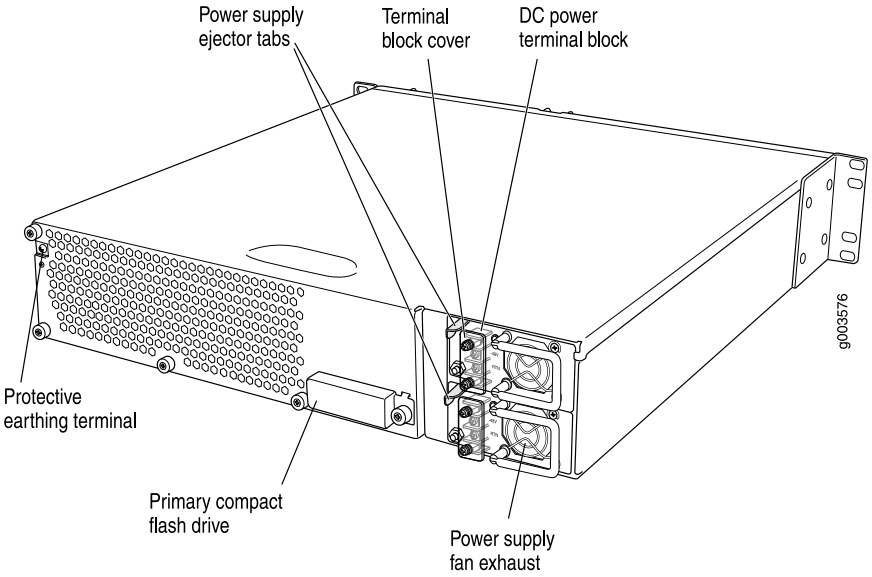


**Figure 12: J4300 and J6300 Hardware Components**

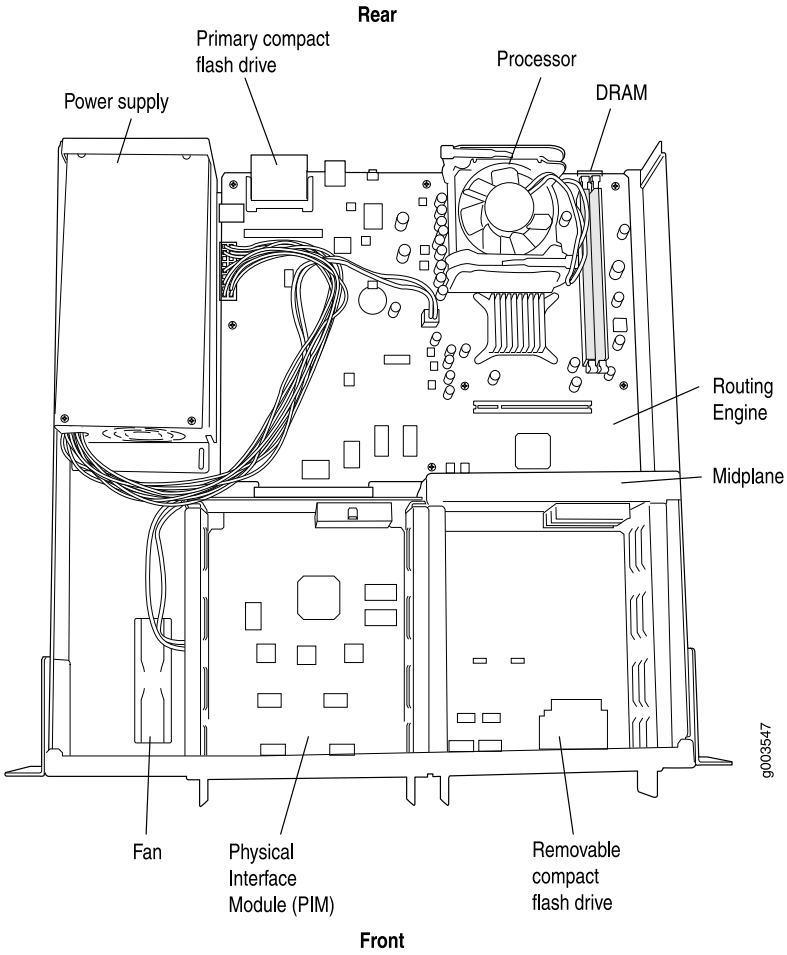



Table 10 on page 24 summarizes the physical specifications for the J4300 and J6300 router chassis.

**Table 10: J4300 and J6300 Physical Specifications**

| Description | Value |
|---|---|
| Chassis dimensions | ■ 3.50 in. (8.9 cm) high<br>■ 17.00 in. (43.2 cm) wide—19 in. (48.3 cm) wide with mounting brackets attached<br>■ 19.00 in. (48.3 cm) deep—plus 0.5 in. (1.27 cm) of hardware that protrudes from the chassis front |
| Router weight | ■ J4300 router minimum configuration (no PIMs): 18 lb (8.2 kg)<br>■ J4300 router maximum configuration (six PIMs): 21 lb (9.5 kg)<br>■ J6300 router minimum configuration (no PIMs and one power supply): 18.5 lb (8.4 kg)<br>■ J6300 router maximum configuration (six PIMs and two power supplies): 24 lb (10.9 kg) |

### *Midplane*

The midplane is located in the center of the chassis and forms the rear of the PIM card cage (see Figure 12 on page 24). 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.

### *J4300 and J6300 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.
- Compact flash drive—Provides primary storage for software images, configuration files, and microcode. The primary compact flash drive is accessible from the rear of the router. For information about replacing the primary compact flash drive, see “Removing and Installing the Primary Compact Flash Disk” on page 148.

**NOTE:** The J4300 and J6300 Services Routers also provide a slot on the front panel in which you can insert an additional removable compact flash. For information about the removable compact flash, see “J4300 and J6300 Removable Compact Flash Drive” on page 28.

#### J4300 and J6300 Boot Devices

The J4300 and J6300 Services Routers can boot from three devices:

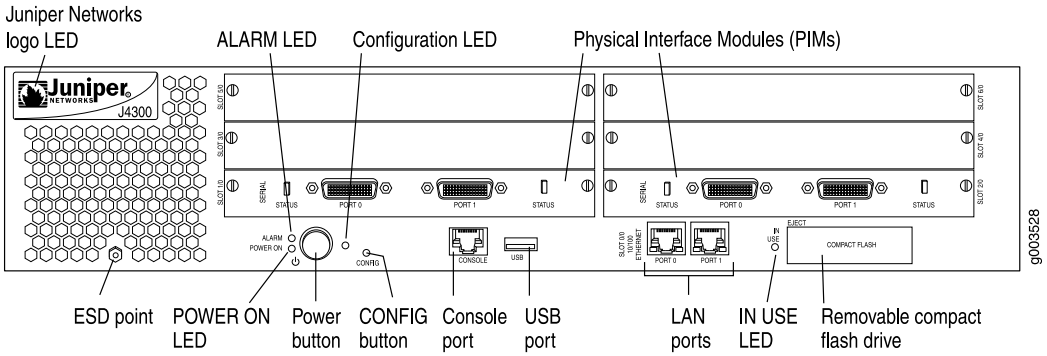
- Primary compact flash disk
- Removable compact flash disk
- USB storage device

Normally, the Services Router boots from the primary compact flash disk. If the compact flash disk fails, the router attempts to boot from the removable compact flash disk, which is the alternate boot device. If the removable compact flash disk is not present or fails, the router attempts to boot from the USB storage device.

## *J4300 and J6300 Front Panel*

The front panel of a J4300 or J6300 Services Router (Figure 13 on page 26) allows you to view router status LEDs, access the console port, connect to LAN ports, and perform simple control functions.

**Figure 13: Front Panel of J4300 and J6300**




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

- Juniper Networks Logo LED on page 27
- ALARM LED on page 27
- Power Button and POWER LED on page 27
- CONFIG Button on page 27
- Console Port on page 27
- USB Port on page 27
- J4300 and J6300 LAN Ports on page 28
- J4300 and J6300 Removable Compact Flash Drive on page 28

### Juniper Networks Logo LED

The Juniper Networks logo LED on J4300 and J6300 Services Routers functions identically to the Juniper Networks logo LED on the J2300 Services Router. See "Juniper Networks Logo LED" on page 15.

### ALARM LED

The ALARM LED on J4300 and J6300 Services Routers functions identically to the ALARM LED on the J2300 Services Router. See "ALARM LED" on page 16.

### Power Button and POWER LED

The power button and POWER LED on J4300 and J6300 Services Routers function identically to the power button and POWER LED on the J2300 Services Router. See "Power Button and POWER LED" on page 16.

### CONFIG Button

The CONFIG button and LED on J4300 and J6300 Services Routers function identically to the CONFIG button and configuration LED on the J2300 Services Router. See "CONFIG Button" on page 17.

### Console Port

You can use the console port on the chassis front panel to connect to the Routing Engine through an RJ-45 serial cable. From the chassis 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 chassis console port, see the *J-series Services Router Administration Guide*.

For pinout information, see "Chassis Console Port Pinouts" on page 185.

### USB Port

The slot labeled USB on the front panel of the J-series Services Router (see Figure 13 on page 26) accepts 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 the USB storage device is installed and configured, it automatically acts as a secondary boot device, if the primary or removable 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.

### J4300 and J6300 LAN Ports

The J4300 and J6300 Services Routers include two fixed 10/100Base-TX Fast Ethernet ports. The LAN ports receive incoming packets from the network and transmit outgoing packets to the network. Each port 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.

The LAN ports are located on the front panel of the router (see Figure 13 on page 26) and are configured like the ports on a Physical Interface Module (PIM). The LAN ports are not field-replaceable. The ports, labeled PORT 0 and PORT 1, correspond to fe-0/0/0 and fe-0/0/1, respectively, for configuration.

For pinouts of Fast Ethernet cable connectors, see "Network Cable Specifications and Connector Pinouts" on page 175.

Each port has two LEDs located on each side of the bottom of the port. Table 9 on page 19 describes the LAN port LEDs.

### J4300 and J6300 Removable Compact Flash Drive

The slot labeled COMPACT FLASH on the front panel of the Services Router (see Figure 13 on page 26) is a removable compact flash drive that accepts a type I or II compact flash disk, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the removable compact flash disk is installed and configured, it automatically acts as the secondary boot device if the primary compact flash drive fails on startup.

Depending on the capacity of the removable compact flash disk, you can also configure it to receive any core files generated during a failure. For information about configuring a removable compact flash disk, see the *J-series Services Router Administration Guide*.

The IN USE LED indicates that the removable compact flash is being accessed. Table 11 on page 28 describes the meaning of the LED states.

**Table 11: IN USE LED**

| Color | State | Description |
|---|---|---|
| Red | On steadily | ■ Router has booted from the removable compact flash drive.<br>■ request system snapshot operation has been executed, and files are being copied to or from the removable compact flash drive.<br>■ Core dump of the kernel is being written to the removable compact flash drive.<br>■ savecore process is retrieving core dump information. |

## J4300 and J6300 Physical Interface Modules (PIMs)

Physical Interface Modules (PIMs) provide the physical connection to various network media types. For more information, see “Field-Replaceable PIMs” on page 47.

For pinouts of PIM cable connectors, see “Network Cable Specifications and Connector Pinouts” on page 175. For PIM replacement instructions, see “Replacing a PIM” on page 144.

## J4300 Power System

The J4300 Services Router uses either AC or DC power. The autosensing power supply (see Figure 8 on page 22 or Figure 9 on page 22) 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. An 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) that requires a dedicated 15 A (–48 VDC) circuit breaker.

For information about site power preparations, see “Power Guidelines, Requirements, and Specifications” on page 83. For information about connecting the router to power and ground, see “Connecting Power” on page 96.

## J6300 Power System

The J6300 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 10 on page 22 or Figure 11 on page 23. The power supplies distribute the different output voltages to the router components, depending on their voltage requirements. When the 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.

Each power supply has an LED located on the power supply faceplate. Table 12 on page 29 describes the J6300 power supply LED.

**Table 12: J6300 Power Supply LED**

| State | Description |
|---|---|
| Off | No power flowing to the power supply. |
| Green | Power supply is working correctly. |
| Red | Power supply is starting up, or has failed. |

For information about site power preparations, see “Power Guidelines, Requirements, and Specifications” on page 83. For information about connecting the router to power and ground, see “Connecting Power” on page 96.

Redundant power supplies on the J6300 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.

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

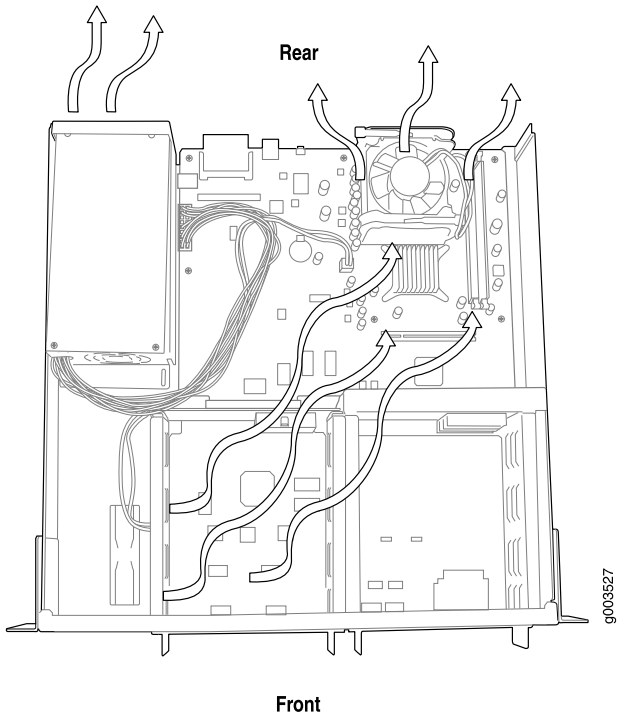
## *J4300 and J6300 Cooling System*

The cooling system includes a fan on the rear of the Routing Engine's processor and a fan at the front of the chassis.

The airflow produced by these fans keeps router components within the acceptable temperature range (see Figure 14 on page 30). The speed of the fan at the rear of the processor is adjusted automatically according to current temperature.

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

**Figure 14: Airflow Through the J4300 and J6300 Chassis**



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.

## 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*

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 “J2300 Routing Engine” on page 14 or “J4300 and J6300 Routing Engine” on page 25.

### *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 13 on page 32 describes the primary JUNOS software processes.

**Table 13: JUNOS Software Processes**

| Process | Name | Description |
|---|---|---|
| Management process | mgd | Manages the Services Router system as follows:<br>■ Provides communication between the other processes and an interface to the configuration database<br>■ Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured<br>■ 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:<br>■ Detects hardware on the system that is used to configure network interfaces<br>■ Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered<br>■ 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. |

**Table 13: JUNOS Software Processes** *(continued)*

| Process | Name | Description |
|---|---|---|
| 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 61.

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 Session and Resource Control (SRC) applications. For more information about these products, see the *JUNOScope Software User Guide* and the *SRC-PE Getting Started Guide*.

Chapter 3

# Physical Interface Modules Overview

J-series Services Routers accept Physical Interface Modules (PIMs) in the slots on the front of the chassis.

**CAUTION:** PIMs are not hot-swappable. You must power off the Services Router before removing or inserting a PIM. Ensure that the PIMs are installed in the router chassis before booting up the system.

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.

For a complete list of supported PIMs, see “Field-Replaceable PIMs” on page 47.

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

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

This chapter contains the following topics.



## PIM Terms

To understand PIMs, become familiar with the terms defined in Table 14 on page 36.

**Table 14: 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. |
| **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).<br><br>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*. |

**Table 14: PIM Terms** *(continued)*

| Term | Definition |
|---|---|
| **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*. |
| **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. |
| **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). |
| **Primary Rate Interface (PRI)** | ISDN service intended for higher-bandwidth applications than ISDN BRI. ISDN PRI consists of a single D-channel for control and signaling, plus a number of 64-Kbps B-channels—either 23 B-channels on a T1 line or 30 B-channels on an E1 line—to carry network traffic. |
| **uPIM** | Universal switching PIM. A particular type of PIM, such as the Gigabit Ethernet uPIM, which can be universally inserted in any slot on a J4350 or J6350 Services Router. |

## J2300 Chassis with Fixed PIMs

The PIMs in J2300 Services Routers are fixed and not interchangeable. All J2300 chassis types have two Fast Ethernet LAN ports and one set of WAN ports. The J2300 Services Routers provide the chassis types summarized in Table 15 on page 38 and described in the following sections:



### *J2300 Chassis PIM Summary*

Table 15 on page 38 provides software release information, port numbers, and sample interface names for J2300 Services Router chassis types.

**Table 15: J2300 Chassis PIM Summary**

| Chassis Type | Software Release | Port Numbering | Sample Interface Names (type–pim/0/port) |
|---|---|---|---|
| Dual-Port Serial | JUNOS 7.0 and later | Ports—0 and 1 for Fast Ethernet interfaces<br><br>Ports—2 and 3 for serial interfaces | fe–0/0/0<br><br>se–0/0/2 |
| Dual-Port Serial with one ISDN BRI port | JUNOS 7.3 and later | Ports—0 and 1 for Fast Ethernet interfaces<br><br>Ports—2 and 3 for serial interfaces<br><br>Port—4 for the ISDN BRI interface | fe–0/0/0<br><br>se–0/0/2<br><br>br–0/0/4 |
| Dual-Port T1 or E1 | JUNOS 7.0 and later | Ports—0 and 1 for Fast Ethernet interfaces<br><br>Ports—2 and 3 for T1 or E1 interfaces | fe–0/0/0<br><br>t1–0/0/2<br><br>e1–0/0/2 |

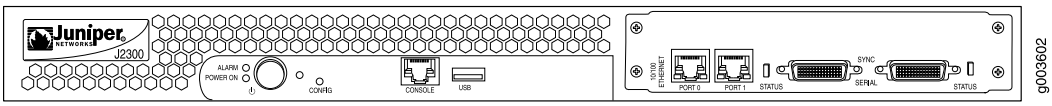
**Table 15: J2300 Chassis PIM Summary** *(continued)*

| Chassis Type | Software Release | Port Numbering | Sample Interface Names (type–pim/0/port) |
|---|---|---|---|
| Dual-Port T1 or E1 with one ISDN BRI port | JUNOS 7.3 and later | Ports—0 and 1 for Fast Ethernet interfaces<br>Ports—2 and 3 for T1 or E1 interfaces<br>Port—4 for the ISDN BRI interface | fe–0/0/0<br>t1–0/0/2<br>e1–0/0/2<br>br–0/0/4 |
| Dual-Port G.SHDSL | JUNOS 7.5 and later | Ports—0 and 1 for Fast Ethernet interfaces<br>Ports—2 and 3 for G.SHDSL interfaces | fe–0/0/0<br>at–0/0/2 |
| Dual-Port G.SHDSL with one ISDN BRI S/T port | JUNOS 7.5 and later | Ports—0 and 1 for Fast Ethernet interfaces<br>Ports—2 and 3 for G.SHDSL interfaces<br>Port—4 for the ISDN BRI S/T interface | fe–0/0/0<br>at–0/0/2<br>br–0/0/4 |

## *Dual-Port Serial Chassis*

The J2300 Dual-Port Serial chassis has two Fast Ethernet LAN ports and two serial WAN ports as shown in Figure 15 on page 39.

**Figure 15: J2300 Serial Chassis**




The Dual-Port Serial chassis 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 the network ports, see “Network Cable Specifications and Connector Pinouts” on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, and Table 17 on page 40 describes the meaning of the status LED for a serial port.

**Table 16: LEDs for Fast Ethernet LAN Ports**

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

**Table 17: Status LED for Serial 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 Serial with ISDN BRI Chassis*

The J2300 Dual-Port Serial with ISDN BRI chassis has two Fast Ethernet LAN ports, two serial WAN ports, and one ISDN BRI U (Figure 16 on page 40) or S/T (Figure 17 on page 40) port. The ISDN BRI interface is the backup interface to the primary serial interface and provides failover support for a serial connection.

**Figure 16: J2300 Serial with ISDN BRI U Chassis**

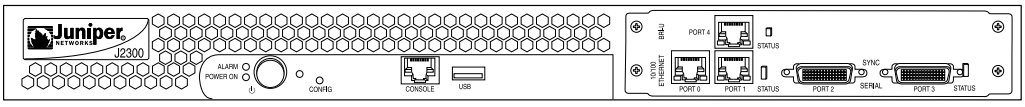
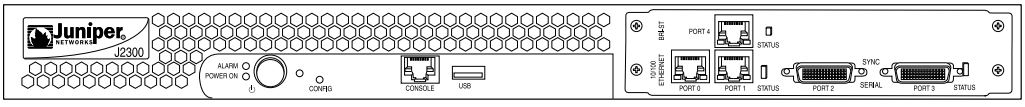



**Figure 17: J2300 Serial with ISDN BRI S/T Chassis**



The serial with ISDN BRI S/T or U interface chassis 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
- Bandwidth on demand
- Dial backup
- Dial-on-demand routing backup

For pinouts of cable connectors for the network ports, see "Network Cable Specifications and Connector Pinouts" on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, Table 18 on page 41 describes the meaning of the status LED for a serial port, and Table 19 on page 41 describes the meaning of the status LED for an ISDN BRI port.

**Table 18: Status LED for Serial 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. |

**Table 19: Status LED for ISDN BRI Port**

| Color | State | Description |
|---|---|---|
| Green | On steadily | PIM is online and operational. |
| Red | Disconnected | PIM is not operational and needs replacement. |
| Unlit | Off | PIM is offline. |

## *Dual-Port T1 or E1 Chassis*

The J2300 Dual-Port T1 or E1 chassis has two Fast Ethernet LAN ports and two T1 or E1 WAN ports. Figure 18 on page 42 shows the E1 chassis, and Figure 19 on page 42 shows the T1 chassis.

**Figure 18: J2300 E1 Chassis**

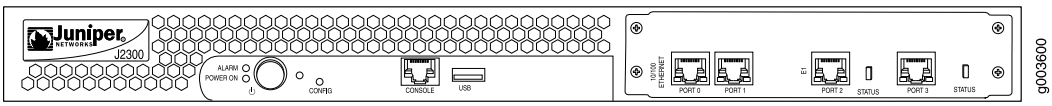
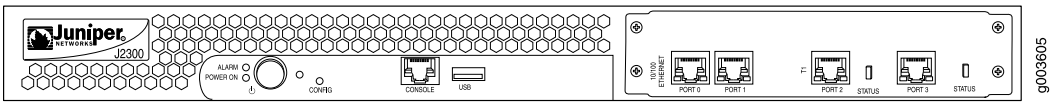



**Figure 19: J2300 T1 Chassis**




The T1 or E1 chassis provides the following key features:

- Onboard network processor
- Integrated CSU/DSU—Eliminates the need for a separate external device
- Framed, unframed (E1 only), and fractional operational modes
- 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
- Local and remote loopback, bit error rate test (BERT), T1 facilities data link (FDL), and long buildout diagnostics

For pinouts of cable connectors for the network ports, see "Network Cable Specifications and Connector Pinouts" on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, and Table 20 on page 42 describes the meaning of the status LED for a T1 or E1 port.

**Table 20: 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 T1 or E1 with ISDN BRI Chassis*

The J2300 Dual-Port T1 or E1 with ISDN BRI chassis has two Fast Ethernet LAN ports, two T1 or E1 WAN ports, and one ISDN BRI port. The ISDN BRI interface is the backup interface to the primary T1 or E1 interface and provides ISDN failover support for a T1 or E1 connection.

The E1 chassis has an ISDN BRI S/T port (Figure 20 on page 43), and the T1 chassis has an ISDN BRI U port (Figure 21 on page 43).

**Figure 20: J2300 E1 with ISDN BRI S/T Chassis**

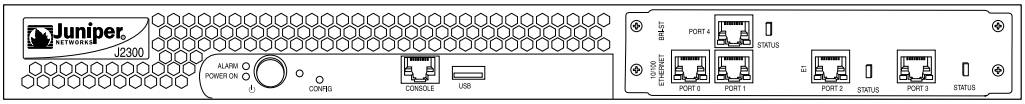
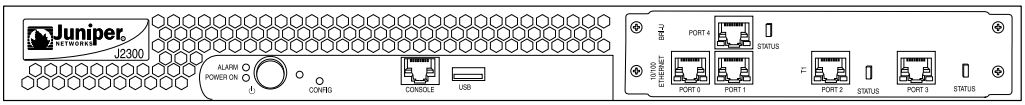



**Figure 21: J2300 T1 with ISDN BRI U Chassis**




The T1 or E1 with ISDN BRI chassis provides the following key features:

- Onboard network processor
- Integrated CSU/DSU—Eliminates the need for a separate external device
- Framed, unframed (E1 only), and fractional operational modes
- 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
- Local and remote loopback, bit error rate test (BERT), T1 facilities data link (FDL), and long buildout diagnostics
- Bandwidth on demand
- Dial backup
- Dial-on-demand routing backup

For pinouts of cable connectors for the network ports, see "Network Cable Specifications and Connector Pinouts" on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, Table 21 on page 44 describes the meaning of the status LED for a T1 or E1 port, and Table 22 on page 44 describes the meaning of the status LED for an ISDN BRI port.

**Table 21: 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. |

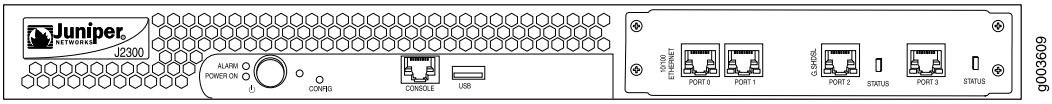
**Table 22: Status LED for ISDN BRI Port**

| Color | State | Description |
|---|---|---|
| Green | On steadily | PIM is online and operational. |
| Red | Disconnected | PIM is not operational and needs replacement. |
| Unlit | Off | PIM is offline. |

## *Dual-Port G.SHDSL Chassis*

The J2300 Dual-Port G.SHDSL chassis has two Fast Ethernet LAN ports and two G.SHDSL WAN ports, as shown in Figure 22 on page 44. The G.SHDSL ports provide symmetric high-speed digital subscriber line (SHDSL) interfaces to ATM network media for ATM-over-SHDSL connections.

**Figure 22: J2300 G.SHDSL Chassis**




The G.SHDSL chassis provides the following key features:

- Onboard network processor
- 2-port two-wire mode and 1-port four-wire mode

**NOTE:** Contact the Juniper Networks Technical Assistance Center (JTAC) before implementing 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.
- Up to 16 virtual channels (VCs) per G.SHDSL port
- 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 the network ports, see “Network Cable Specifications and Connector Pinouts” on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, and Table 23 on page 45 describes the meaning of the status LED for a G.SHDSL port.

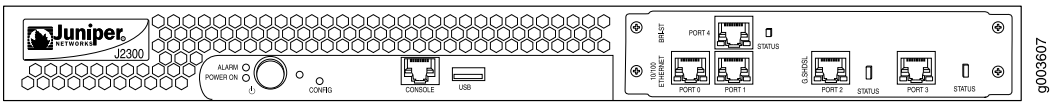
**Table 23: Status LED for G.SHDSL Ports**

| 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. |

## *Dual-Port G.SHDSL with ISDN BRI S/T Chassis*

The J2300 Dual-Port G.SHDSL with ISDN BRI chassis has two Fast Ethernet LAN ports, two G.SHDSL WAN ports, and one ISDN BRI S/T port as shown in Figure 23 on page 45. The G.SHDSL ports provide symmetric high-speed digital subscriber line (SHDSL) interfaces to ATM network media for ATM-over-SHDSL connections. The ISDN BRI S/T interface is the backup interface to the primary G.SHDSL interface and provides ISDN failover support for a G.SHDSL connection.

**Figure 23: J2300 G.SHDSL with ISDN BRI S/T Chassis**




The G.SHDSL with ISDN BRI S/T chassis provides the following key features:

- Onboard network processor
- 2-port two-wire mode and 1-port four-wire mode

**NOTE:** Contact the Juniper Networks Technical Assistance Center (JTAC) before implementing 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.
- Up to 16 virtual channels (VCs) per G.SHDSL port
- 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
- Bandwidth on demand
- Dial backup
- Dial-on-demand routing backup

For pinouts of cable connectors for the network ports, see "Network Cable Specifications and Connector Pinouts" on page 175.

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

Table 16 on page 40 describes the meaning of the LEDs for a Fast Ethernet port, Table 24 on page 46 describes the meaning of the status LED for a G.SHDSL port, and Table 25 on page 46 describes the meaning of the status LED for an ISDN BRI port.

**Table 24: Status LEDs for G.SHDSL 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 25: Status LED for ISDN BRI Port**

| Color | State | Description |
|---|---|---|
| Green | On steadily | PIM is online and operational. |
| Red | Disconnected | PIM is not operational and needs replacement. |

**Table 25: Status LED for ISDN BRI Port** *(continued)*

| Color | State | Description |
|---|---|---|
| Unlit | Off | PIM is offline. |

## 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 26 on page 47 and described in the following sections:

- J4300 and J6300 Field-Replaceable PIM Summary on page 47
- Dual-Port Serial PIM on page 48
- Dual-Port T1 or E1 PIM on page 49
- Dual-Port Channelized T1/E1/ISDN PRI PIM on page 51
- T3 or E3 PIM on page 53
- Dual-Port Fast Ethernet PIM on page 54
- 4-Port ISDN BRI PIMs on page 55
- ADSL PIM on page 56
- G.SHDSL PIM on page 58

### *J4300 and J6300 Field-Replaceable PIM Summary*

Table 26 on page 47 provides software release information, slot and port numbers, and sample interface names for the field-replaceable PIMs supported on J4300 and J6300 Services Routers.

**Table 26: J4300 and J6300 Field-Replaceable PIM Summary**

| PIM | Software Release | Slot and Port Numbering | Sample Interface Name (type-pim/0/port) |
|---|---|---|---|
| Dual-Port Serial | JUNOS 7.0 and later | Slots—1 through 6<br>Ports—0 and 1 | se-3/0/1 |

**Table 26: J4300 and J6300 Field-Replaceable PIM Summary** *(continued)*

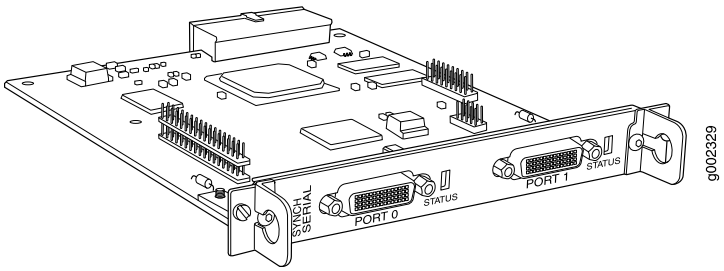
| PIM | Software Release | Slot and Port Numbering | Sample Interface Name (type-pim/0/port) |
|---|---|---|---|
| Dual-Port T1 or E1 | JUNOS 7.0 and later | Slots—1 through 6<br>Ports—0 and 1 | t1-0/0/1<br>or<br>e1-0/0/1 |
| Dual-Port Channelized T1 or E1 | JUNOS 8.1 and later | Slots—1 through 6<br>Port—0 and 1 | ct1-3/0/0<br>ce1-3/0/0 |
| T3 or E3 | T3 PIM—JUNOS 7.0 and later<br>E3 PIM—JUNOS 7.3 and later | Slots—1 through 6<br>Port—0 | t3-0/0/0<br>or<br>e3-2/0/0 |
| Dual-Port Fast Ethernet | JUNOS 7.0 and later | Slots—1 through 6<br>Ports—0 and 1 | fe-1/0/0 |
| 4-Port ISDN BRI | JUNOS 7.3 and later | Slots—1 through 6<br>Ports—0, 1, 2, and 3 | br-1/0/2 |
| ADSL | ADSL Annex A and Annex B—JUNOS 7.2 and later<br>ADSL 2/2+ Annex A—JUNOS 7.3 and later<br>ADSL 2/2+ Annex B—JUNOS 7.4 and later | Slots—1 through 6<br>Port—0 | at-2/0/0 |
| G.SHDSL | JUNOS 7.4 and later | Slots—1 through 6<br>Ports—0 and 1 | at-1/0/0 |

**NOTE:** PIMs are not hot-swappable. PIMs must be installed in front panel slots before the system is booted up.

## *Dual-Port Serial PIM*

The Dual-Port Serial PIM (Figure 24 on page 49) provides a physical connection to serial network media types through two serial interface ports.

**Figure 24: 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 175.

To install or remove a PIM, see "Replacing a PIM" on page 144.

Status LEDs indicate port status. Table 27 on page 49 describes the meaning of the LED states.

**Table 27: Status LEDs for Serial 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. |

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

## *Dual-Port T1 or E1 PIM*

The Dual-Port T1 PIM (Figure 25 on page 50) and Dual-Port E1 PIM (Figure 26 on page 50) 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 25: Dual-Port T1 PIM**

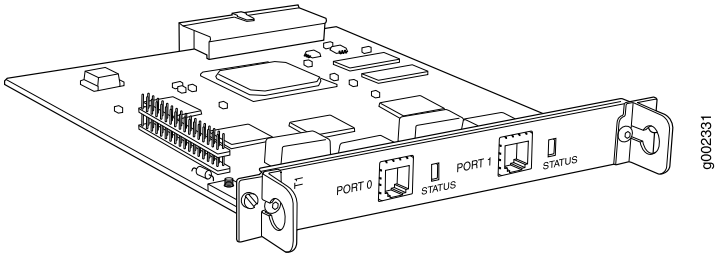
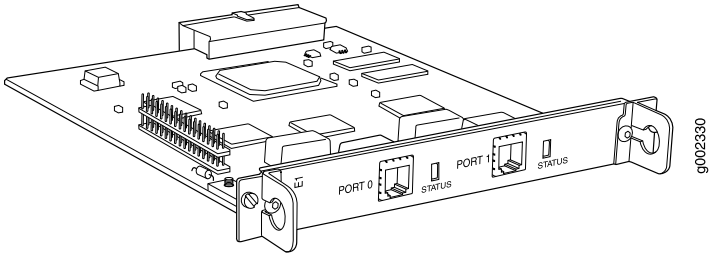



**Figure 26: Dual-Port E1 PIM**




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 186.

To install or remove a PIM, see “Replacing a PIM” on page 144.

Status LEDs indicate port status. Table 28 on page 50 describes the meaning of the LED states.

**Table 28: 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. |

**Table 28: Status LEDs for T1 and E1 Ports** *(continued)*

| Color | State | Description |
|---|---|---|
| Unlit | Off | Offline. |

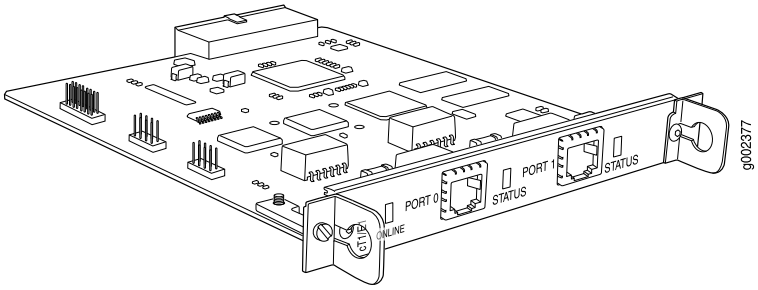
For alarms, see the configuring and monitoring alarms information in the *J-series Services Router Administration Guide*.

## *Dual-Port Channelized T1/E1/ISDN PRI PIM*

The Dual-Port Channelized T1/E1/ISDN PRI PIM (Figure 27 on page 51) is a multiflex interface card that allows you to configure a single interface as a channelized T1 interface or a channelized E1 interface. You can also configure ISDN PRI services on a channelized T1 or E1 interface. The channelized T1/E1/ISDN PRI interface supports up to 24 DS0 channels on a T1 interface and up to 31 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/E1/ISDN PRI interface through a J-Web Quick Configuration page.

**Figure 27: Channelized T1/E1/ISDN PRI PIM**




The Dual-Port Channelized T1/E1/ISDN PRI PIM provides the following key features:

- Onboard network processor
- Two-port channelization
- Interfaces that are software configurable as T1 or E1 channels or ISDN PRI B-channels
- 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) and 4098 bytes (for ISDN PRI services)

**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/E1/ISDN PRI PIMs, see "ISDN RJ-45 Connector Pinout" on page 190.

To install or remove a PIM, see "Replacing a PIM" on page 144.

Channelized T1/E1/ISDN PRI LEDs indicate PIM and port status. Table 29 on page 52 describes the meaning of the LED states.

**NOTE:** The STATUS LED displays channelized T1 or E1 port activity and alarms only. It does not display ISDN PRI B-channel or D-channel status.

**Table 29: LEDs for Channelized T1/E1/ISDN PRI 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. |

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

## *T3 or E3 PIM*

The T3 (also known as DS3) PIM (Figure 28 on page 53) and E3 PIM (Figure 29 on page 53) are supported on J6300 Services Routers and 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 28: T3 PIM**

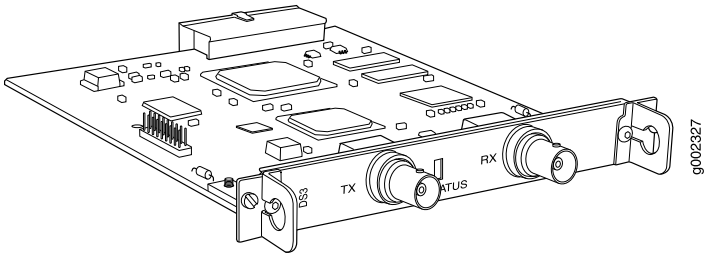
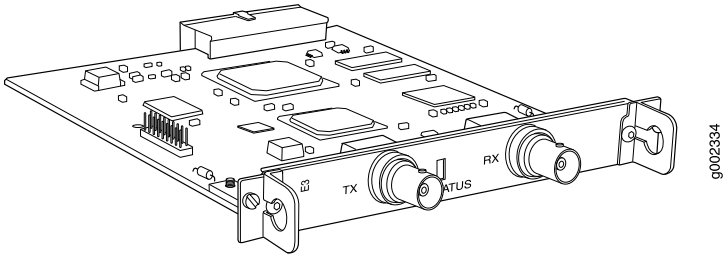



**Figure 29: E3 PIM**




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 189.

To install or remove a PIM, see "Replacing a PIM" on page 144.

Status LEDs indicate port status. Table 30 on page 54 describes the meaning of the LED states.

**Table 30: Status LEDs for T3 and E3 Ports**

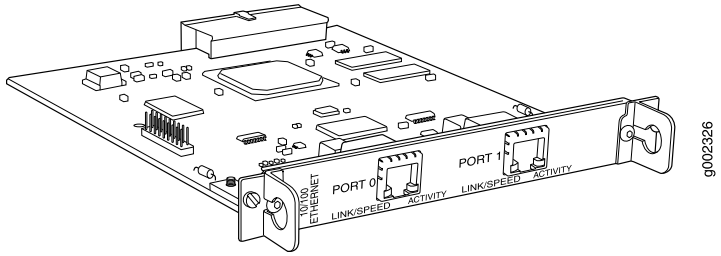
| Color | State | Description |
|---|---|---|
| Green | On steadily | Online with no alarms or failures. |
| Red | On steadily | Active with a local alarm. The router has detected a failure. |
| Yellow | On steadily | ■ Loopback mode.<br>■ T3 (DS3)—Remote endpoint is in red alarm failure.<br>■ E3—Remote defect indication (RDI). |
| Unlit | Off | Offline. |

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

## *Dual-Port Fast Ethernet PIM*

The Dual-Port 10/100-Mbps Fast Ethernet PIM (Figure 30 on page 54) has two physical Fast Ethernet ports.

**Figure 30: 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 “Fast Ethernet RJ-45 Connector Pinout” on page 185.

To install or remove a PIM, see “Replacing a PIM” on page 144.

Fast Ethernet LEDs indicate link status, port speed, and activity. Table 31 on page 55 describes the meaning of the LEDs.

**Table 31: LEDs for Dual-Port Fast Ethernet PIM**

| Label | Color | State | Description |
|---|---|---|---|
| LINK/SPEED | Green (100 Mbps)<br>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. |

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

## *4-Port ISDN BRI PIMs*

The 4-port ISDN BRI PIMs have four physical ports that support the ISDN BRI S/T (Figure 31 on page 55) or ISDN BRI U (Figure 32 on page 55) interface type.

**Figure 31: ISDN BRI S/T PIM**

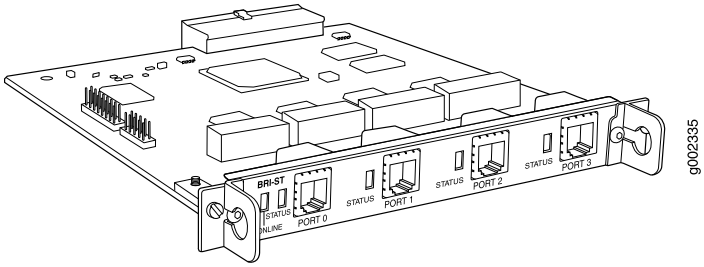
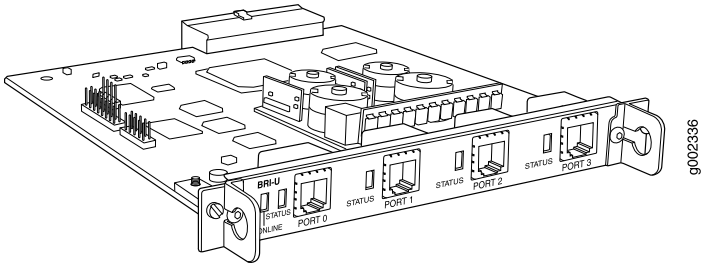



**Figure 32: ISDN BRI U PIM**




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 190.

To install or remove a PIM, see "Replacing a PIM" on page 144.

ISDN LEDs indicate PIM and port status. Table 32 on page 56 describes the meaning of the LED states.

**Table 32: 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.<br>■ ISDN Layer 2 is unavailable. |
| | Red | Disconnected | ■ BRI interface port is not connected.<br>■ 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. |

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

## *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 33 on page 57) over plain old telephone service (POTS) and the other Annex B (Figure 34 on page 57) over ISDN, includes one physical ADSL port for an ATM-over-ADSL connection.

**Figure 33: ADSL 2/2+ Annex A PIM**

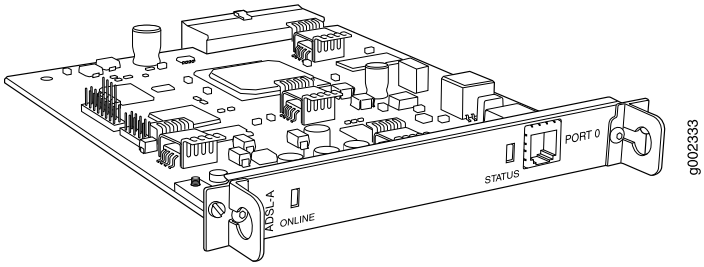
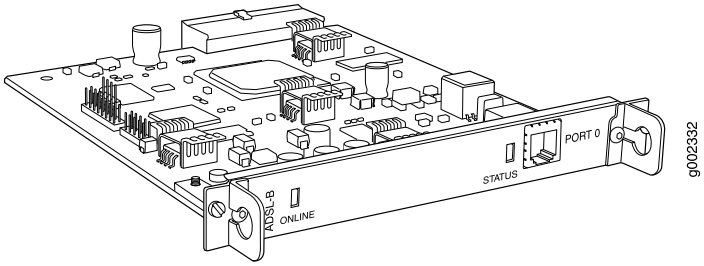



**Figure 34: ADSL 2/2+ Annex B PIM**




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 189.

To install or remove 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 33 on page 57 describes the meaning of the LED states.

**Table 33: LEDs for ADSL PIMs**

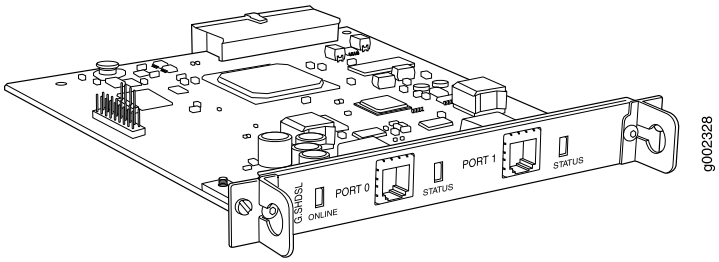
| Label | Color | State | Description |
|---|---|---|---|
| ONLINE | Green | On steadily | PIM passed the self-test and is online and operational. |
| | Unlit | Off | PIM is offline. |
| STATUS | Green | On steadily | Online with no alarms or failures. |
| | Red | On steadily | Active with local or remote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

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

## G.SHDSL PIM

The G.SHDSL PIM (Figure 35 on page 58) 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 35: 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

**NOTE:** Payload loopback functionality is not supported on ATM-over-SHDSL interfaces.

For pinouts of cable connectors for G.SHDSL PIMs, see "ADSL and G.SHDSL RJ-11 Connector Pinout" on page 189.

To install or remove 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 34 on page 59 describes the meaning of the LED states.

**Table 34: 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. |

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

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

This section contains the following topics:



### *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 62.

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 64.

### 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 62.

For more information about the CLI, see "Using the Command-Line Interface" on page 68.

### Comparison of Configuration Interfaces

Table 35 on page 63 describes and compares the interfaces you can use to configure a Services Router.

**Table 35: 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.<br><br>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:<br>■ Setup<br>■ Secure access<br>■ Interfaces<br>■ User access<br>■ SNMP notifications<br>■ Routing and protocols, including data link switching (DLSw)<br>■ Class of service (CoS)<br>■ Security firewall filters and Network Address Translation (NAT)<br>■ Dynamic Host Configuration Protocol (DHCP) services<br>■ IPSec tunnels<br>■ Real-time performance monitoring<br>■ Input and output firewall filters (ACLs) | Use for basic configuration. |
| J-Web configuration editor | Web browser pages divided into panes in which you can do any of the following:<br>■ 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.<br>■ Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines.<br>■ Upload or download a complete configuration.<br>■ Roll back to a previous configuration.<br>■ Create or delete a rescue configuration. | Configure all router services:<br>■ System parameters<br>■ User access and accounting<br>■ Interfaces<br>■ SNMP network management<br>■ Routing options, including multicast routing<br>■ Routing protocols<br>■ Routing policies<br>■ Secure access<br>■ Service interfaces, including stateful firewalls and virtual private networks (VPNs)<br>■ Traffic engineering, including Multiprotocol Label Switching (MPLS) and class-of-service (CoS) packet prioritization<br>■ 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:<br>■ Type commands on a line and press Enter to create a hierarchy of configuration statements.<br>■ Create an ASCII text file that contains the statement hierarchy.<br>■ Upload a complete configuration, or roll back to a previous configuration.<br>■ 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 103. 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*

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 36 on page 65) 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 36 on page 65 and Figure 37 on page 66:

- 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 36 on page 66 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 36: J-Web Layout**

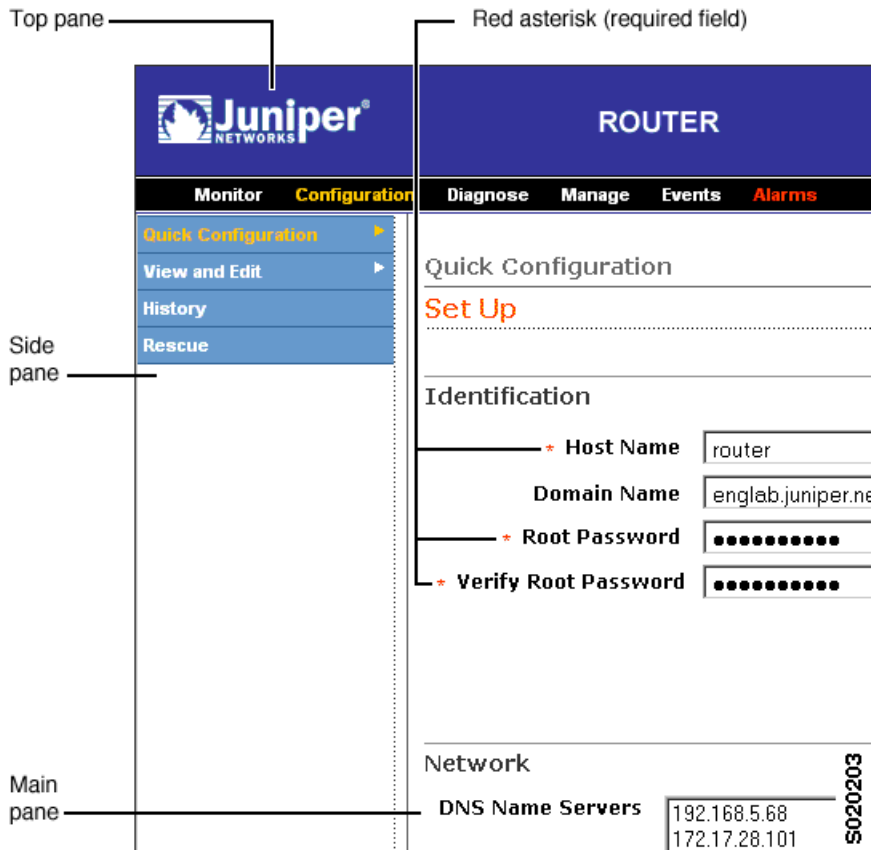


**Figure 37: J-Web Layout—Configuration Editor**

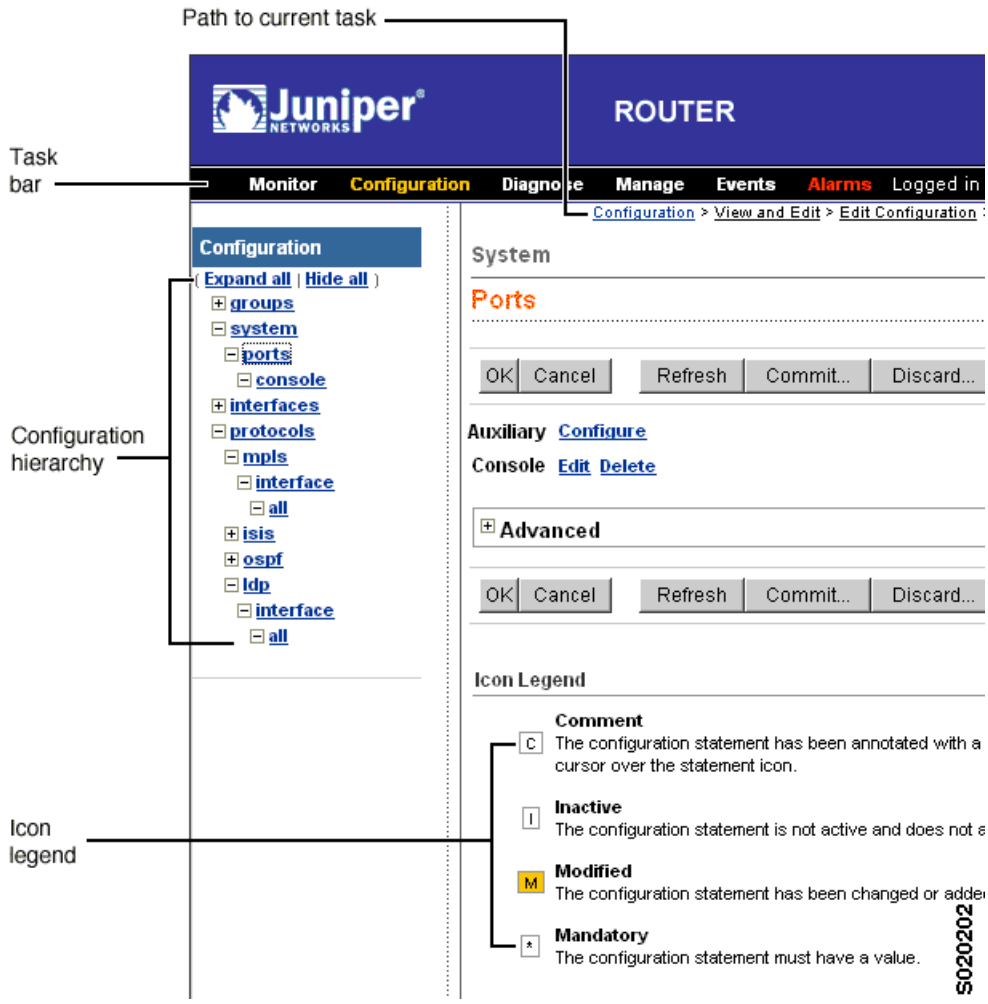



**Table 36: Summary of J-Web Elements**

| 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. |

**Table 36: Summary of J-Web Elements** *(continued)*

| J-Web Interface Element | Description |
|---|---|
| Task bar | Menu of J-Web main options. Click to access.<br>■ **Monitor**—View information about configuration and hardware on the Services Router.<br>■ **Configuration**—Configure the Services Router with Quick Configuration or the configuration editor, and view configuration history.<br>■ **Diagnose**—Troubleshoot network connectivity problems.<br>■ **Manage**—Manage files and licenses, upgrade software, and reboot the Services Router.<br>■ **Events**—View events and set up filters for an event summary.<br>■ **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:<br>■ C—Comment. Move your cursor over the icon to view a comment about the configuration statement.<br>■ I—Inactive. The configuration statement does not affect the Services Router.<br>■ M—Modified. The configuration statement is added or modified.<br>■ *—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.<br>■ Click **Expand all** to display the entire hierarchy.<br>■ Click **Hide all** to display only the statements at the top level.<br>■ Click plus signs (+) to expand individual items.<br>■ 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:

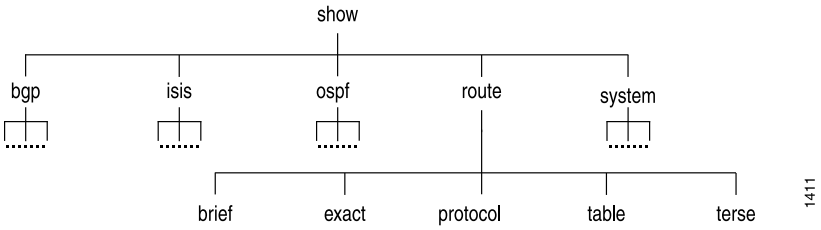


For more information about the CLI, see the *JUNOS CLI User Guide*.

### *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 38 on page 68 illustrates a portion of the show command hierarchy.

**Figure 38: 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.
   - To access the router through the J-Web interface, select **Diagnose > CLI Terminal** in the J-Web interface. For more information, see the *J-Web Interface User Guide*.
2. Log in using your username and password.

   After you log in, you enter a UNIX shell.
3. Start the CLI.

```
% 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 routing platform.

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 74. To enter configuration mode, see "CLI Configuration Mode" on page 70. 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

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 37 on page 72 lists some typical CLI editing tasks and the keystrokes that perform them.

**Table 37: 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 |
| 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 69 and "CLI Configuration Mode" on page 70.
- 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 38 on page 74, 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 38: help Commands**

| CLI Command | Description |
|---|---|
| help apropos *string* | Displays help based on a text string contained in a statement or command name.<br><br>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.<br><br>In configuration mode, this command displays statement names and help text that match the string specified.<br><br>In operational mode, this command displays the following types of commands that match the string specified, plus help text:<br>■ Operational mode commands<br>■ help topic and help reference commands you can enter for more information<br><br>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.<br><br>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.<br><br>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 39 on page 75 shows how you can change the CLI environment features.

**Table 39: 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.<br>■ 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.<br>■ 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.<br>■ Set on to reenable the prompt. |

**Table 39: Configuring the CLI Environment** *(continued)*

| Environment Feature | CLI Command | Default Setting | Options |
|---|---|---|---|
| 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.<br>■ 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.) |
| 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:<br>■ ansi<br>■ vt100<br>■ small-xterm<br>■ xterm |

# Part 2
# Installing a Services Router

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

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 195, 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.

## Desktop and Wall Mounting Requirements

The J2300 Services Router can be installed on a desktop or wall. When choosing a location, allow at least 6 in. (15.2 cm) of clearance between the front and back of the chassis and adjacent equipment or walls.

If you are mounting the J2300 router on a wall, use wall screws or wall anchors capable of supporting the full weight of the chassis, up to 12 lb (5.4 kg). If possible, install the wall anchors into wall studs, which provide added support for the chassis.

## Rack Requirements

All J-series Services Routers can be installed in a rack. J4300 and J6300 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 80
- Connection to Building Structure on page 81


### *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

- A J2300 chassis is 1.75 in. (4.4 cm) high, 17.25 in. (43.8 cm) wide, and 12.37 in. (31.4 cm) deep.
- A J4300 or J6300 chassis is 3.5 in. (8.9 cm) high, 17 in. (43.2 cm) wide, and 19 in. (48.3 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 79.)

**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 J2300 chassis height of 1.75 in. (4.4 cm) equals 1 U. The J4300 and J6300 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 211.

## Router Environmental Tolerances

Table 40 on page 81 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 40: 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 0°C (32°F) to 40°C (104°F)<br><br>Non-operating storage temperature in shipping carton: 40°C (–40°F) to 70°C (158°F) |
| Seismic | Designed to meet Telcordia Technologies Zone 4 earthquake requirements |

**Table 40: Router Environmental Tolerances** *(continued)*

| Description | Value |
|---|---|
| Maximum thermal output | J2300 chassis<br>■ Typical—270 BTU/hour (80 W)<br>■ Maximum—750 BTU/hour (220 W)<br><br>J4300 and J6300 chassis<br>■ Typical—510 BTU/hour (150 W)<br>■ Maximum—1190 BTU/hour (350 W) |

## Spacing of Mounting Holes

The mounting holes in the mounting brackets provided with the J2300 Services Router chassis are spaced 1.25 in. (3.2 cm) apart, measured from the center of the hole.

The mounting holes in the mounting brackets attached to the J4300 and J6300 chassis are spaced in two groups. The space between the holes in each group is 0.6 in. (1.5 cm) apart, measured from the center of each hole. The space between the two groups is 1.75 (4.4 cm) apart, measured from the center of the lower hole in the top group to the upper hole in the bottom group.

## 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 102.)

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 83.

### *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 “J2300 Power System” on page 19, “J4300 Power System” on page 29, and “J6300 Power System” on page 29.

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



### *Site Electrical Wiring Guidelines*

**WARNING:** DC-powered J2300 Services Routers are intended for installation in a dedicated equipment room where they are accessible by trained personnel only. DC-powered J4300 and J6300 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 41 on page 84 lists the AC and DC power system electrical specifications for J-series Services Routers.

**Table 41: AC and DC Power System Electrical Specifications**

| Item | Specification |
|---|---|
| AC input voltage | 100 to 240 VAC nominal<br>100 to 264 VAC operating range (J2300, J4300, and J6300 Services Routers) |
| AC input line frequency | 47 to 63 Hz (J2300, J4300, and J6300 Services Routers)<br>50 to 60 Hz (J4350 and J6350 Services Routers) |

**Table 41: AC and DC Power System Electrical Specifications** *(continued)*

| Item | Specification |
|---|---|
| AC system current rating | 4 to 2 A (J2300 Services Router)<br>6 to 3 A (J4300 and J6300 Services Routers)<br>6 A (J4350 Services Router)<br>8 A (J6350 Services Router) |
| DC input voltage | –42 to –72 VDC operating range (J2300, J4300, and J6300 Services Routers)<br>–48 to –60 VDC operating range (J4350 and J6350 Services Routers) |
| DC system current rating | 4 A @ –48 VDC (nominal, J2300 Services Router)<br>8 A @ –48 VDC (nominal, J4300 and J6300 Services Routers)<br>20 A ((J4350 and J6350 Services Routers) |

## *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 42 on page 85 lists AC power cord specifications provided for each country or region.

**Table 42: AC Power Cord Specifications**

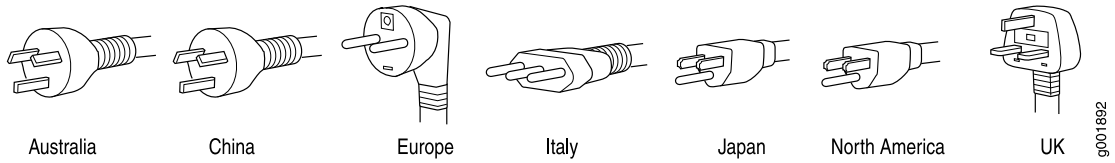
| Country | Electrical Specifications | Plug Standards |
|---|---|---|
| Australia | 250 VAC, 10 A, 50 Hz | AS/NZ 3112–1993 |
| China | 250 VAC, 10 A, 50 Hz | GB2099.1 1996 and GB1002 1996 (CH1-10P) |

**Table 42: 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 39 on page 86 illustrates the plug on the power cord for each country or region listed in Table 42 on page 85.

**Figure 39: 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 "J2300 Power System" on page 19, "J4300 Power System" on page 29, or "J6300 Power System" on page 29.

To connect the power cord during initial installation, see "Connecting Power" on page 96.

To replace the AC power cord, see "Replacing an AC Power Supply Cord" on page 158.

## *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 J6300 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:** You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. 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.

**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 "J2300 Power System" on page 19, "J4300 Power System" on page 29, or "J6300 Power System" on page 29.

To connect the DC power cable during initial installation, see "Connecting DC Power" on page 98.

To replace a DC power cable, see "Replacing a DC Power Supply Cable" on page 161.

## 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 175.

## 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 43 on page 88 summarizes the tasks you need to perform when preparing a site for Services Router installation.

**Table 43: 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

Before you begin installation, complete the following tasks:

- Read the information in "Maintenance and Operational Safety Guidelines and Warnings" on page 219, with particular attention to "Chassis Lifting Guidelines" on page 210.
- 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 79.
- For installation, gather the equipment and tools listed in Table 44 on page 90.

**Table 44: Equipment and Tools Required for Services Router Installation**

| Desk Installation—J2300 Services Router Only | Wall Installation—J2300 Services Router Only | Rack Installation |
|---|---|---|
| Rubber feet (provided) | ■ Rubber feet (provided)<br>■ Mounting brackets and screws (provided)<br>■ Number 2 Phillips screwdriver<br>■ Four wall screws or four mounting screws and anchors capable of supporting the full weight of the chassis, up to 12 lb (5.4 kg) | ■ Mounting brackets and screws (provided)<br>■ Number 2 Phillips screwdriver<br>■ Four (J2300) or eight (J4300 and J6300) mounting screws appropriate for your rack |

- 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 grounding cable and lug, as specified in "Chassis Grounding" on page 96, and the power cords or cords shipped with the router. (You must supply your own power cables if you have a DC-powered router. See "DC Power, Connection, and Power Cable Specifications" on page 86.)

**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 175.
- 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 87.

## 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. Save the shipping carton and packing materials in case you later need to move or ship the router.

## Installing the J2300 Services Router

**WARNING:** DC-powered J2300 Services Routers are intended for installation in a dedicated equipment room where they are accessible by trained personnel only.

You can install the J2300 Services Router on a desk, on a wall, or in a rack. The J2300 Services Router includes mounting brackets that support either wall or rack mounting, and rubber feet for desk and wall mounting.

Install the J2300 Services Router as appropriate for your site, with one of the following procedures:

- Installing the J2300 Services Router on a Desk on page 91
- Installing the J2300 Services Router on a Wall on page 92
- Installing the J2300 Services Router into a Rack on page 93

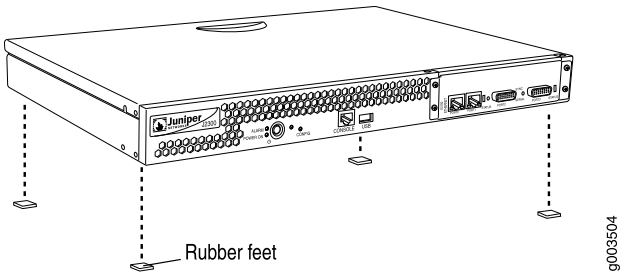
### *Installing the J2300 Services Router on a Desk*

You can install the J2300 Services Router on a desk, table, or other level surface. The router is shipped with rubber feet in the accessory box. The rubber feet are necessary to stabilize the router on the desk.

To install the J2300 router on a desk:

1. Turn the chassis upside-down on the desk or work surface where you intend to operate the router.
2. Attach the provided rubber feet to the bottom of the chassis, as shown in Figure 40 on page 92.
3. Turn the chassis right-side up on the desk or work surface.

**Figure 40: Attaching Rubber Feet to the J2300 Services Router**




## *Installing the J2300 Services Router on a Wall*

You can install the J2300 Services Router on a wall. The router is shipped with mounting brackets and rubber feet in the accessory box. The rubber feet help stabilize the router on the wall and enhance airflow.

To install the J2300 router on a wall:

1. Turn the chassis upside-down on a desk or work surface near where you intend to operate the router.
2. Attach the provided rubber feet to the bottom of the chassis, as shown in Figure 40 on page 92.
3. Turn the chassis right-side up, and place it on a flat surface.
4. Position a mounting bracket on each side of the chassis as shown in Figure 41 on page 93.
5. Use a number 2 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.
6. If you are using wall anchors to support the chassis, install two pairs of anchors on the wall, spaced 19 in. (48.3 cm) apart.

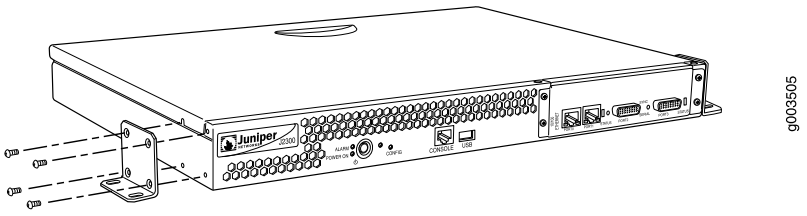
---

**CAUTION:** Mounting screws and wall anchors must be strong enough to support the full weight of the chassis, up to 12 lb (5.4 kg). Attaching the router to wall studs or using wall anchors provides extra support for the chassis.

---

7. Have one person grasp the sides of the router, lift the router, and position it on the wall.
8. Have a second person install two pairs of mounting screws through the bracket holes on either side of the router, to secure the router to the wall.
9. Verify that the mounting screws on one side are aligned with the mounting screws on the opposite side and that the router is level.

**Figure 41: Attaching Mounting Brackets to Install a J2300 Services Router on a Wall**




## *Installing the J2300 Services Router into a Rack*

You can front-mount the J2300 Services Router in a rack. The router is shipped with mounting brackets in the accessory box. 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 80.

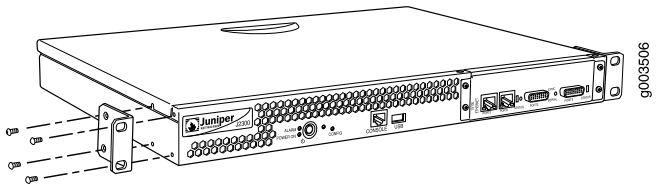
**NOTE:** If you are installing multiple routers in one rack, install the lowest one first and proceed upward in the rack.

**NOTE:** The chassis weighs up to 12 lb (5.4 kg). Have one person lift the chassis into the rack and a second person secure the mounting screws.

To install the J2300 router into a rack:

1. Position a mounting bracket on each side of the chassis as shown in Figure 42 on page 94.
2. Use a number 2 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.
3. Have one person grasp the sides of the router, lift the router, and position it in the rack.
4. Align the bottom hole in each mounting bracket with a hole in each rack rail, making sure the chassis is level.
5. Have a second person install a mounting screw into each of the two aligned holes. Use a number 2 Phillips screwdriver to tighten the screws.
6. Install the second screw in each mounting bracket.
7. 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.

**Figure 42: Attaching Mounting Brackets to Install a J2300 Services Router in a Rack**




## Installing the J4300 or J6300 Services Router

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

You can front-mount the J4300 or J6300 Services Router in a rack. 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 80.

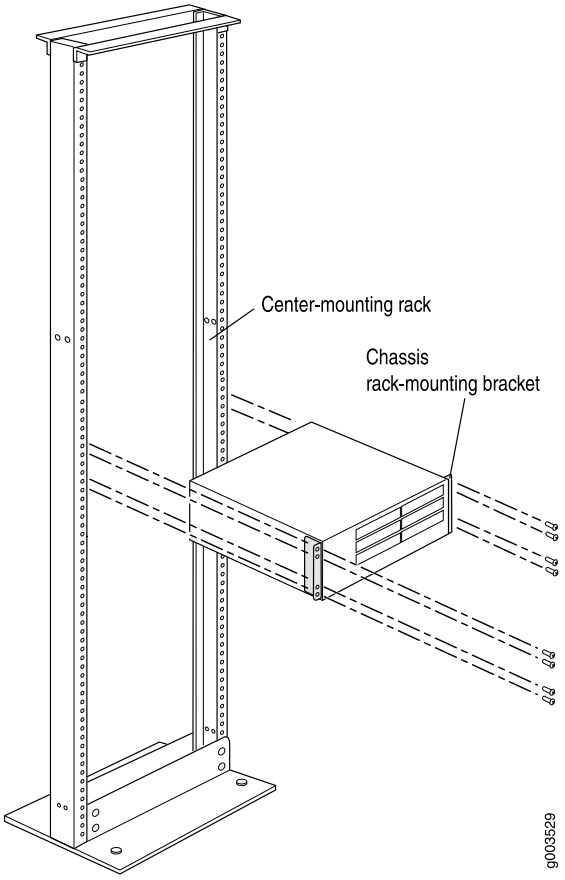
**WARNING:** If you are installing multiple routers in one rack, install the lowest one first and proceed upward in the rack. Install heavier routers in the lower part of the rack. The router should be mounted at the bottom of the rack if it is the only unit in the rack.

**NOTE:** The chassis weighs between 18 lb (8 kg) and 31 lb (14 kg). Have one person lift the chassis into the rack and a second person secure the mounting screws.

To install the J4300 or J6300 router into a rack:

1. Have one person grasp the sides of the router, lift the router, and position it in the rack.
2. Align the bottom hole in each mounting bracket with a hole in each rack rail as shown in Figure 43 on page 95, making sure the chassis is level.
3. Have a second person install a mounting screw into each of the two aligned holes. Use a number 2 Phillips screwdriver to tighten the screws.
4. Install the remaining screws in each mounting bracket.
5. 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.

**Figure 43: Installing the J4300 or J6300 Services Router**




## 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 175.
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 the following amperage:

- J2300 router—up to 4 A
- J4300 router and J6300 router—up to 8 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 96.)

## Connecting Power

J2300 or J4300 Services Routers have a single fixed power supply. J6300 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 83.

**WARNING:** DC-powered J2300 Services Routers are intended for installation in a dedicated equipment room where they are accessible by trained personnel only. 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 85

To connect AC power to the router:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 195.
2. Use a grounding cable to connect the router to earth ground: (For cable requirements, see “Chassis Grounding” on page 96.)
    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 screw and washer from the PEM nut 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 44 on page 97, Figure 45 on page 98, and Figure 46 on page 98.
    e. Secure the cable lug to the grounding point, first with the washer, then with the screw.
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 83.
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 44 on page 97, Figure 45 on page 98, and Figure 46 on page 98.
    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 44: Connecting AC Power to the J2300 Services Router**

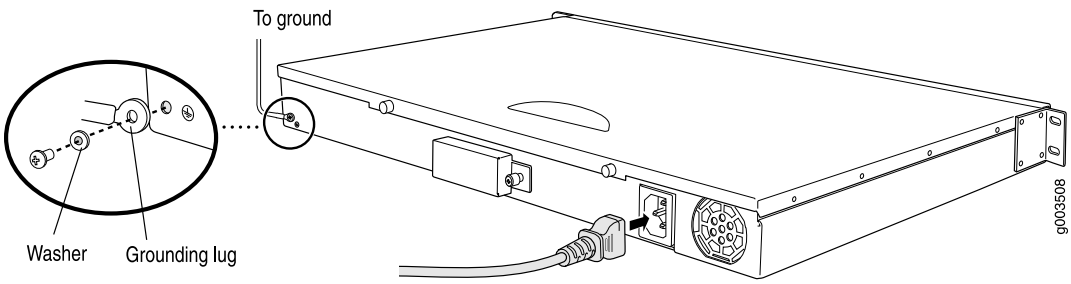


**Figure 45: Connecting AC Power to the J4300 Services Router**

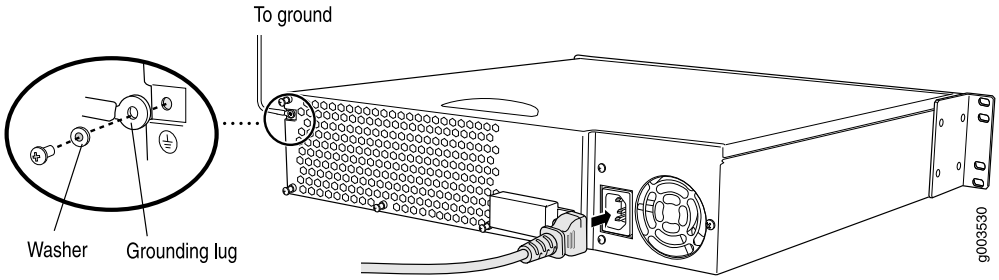
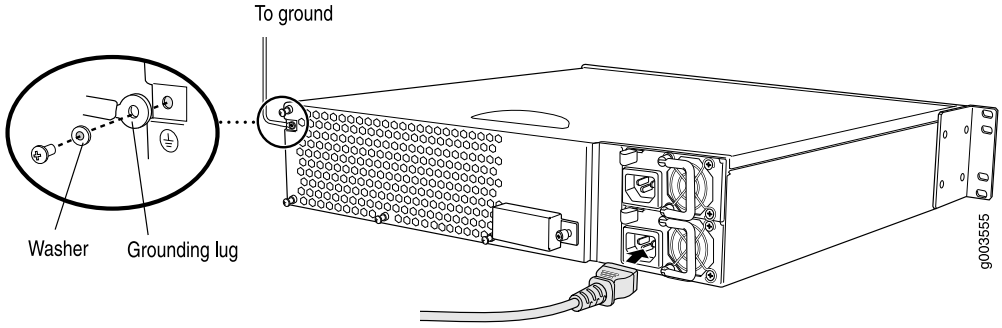



**Figure 46: Connecting AC Power to the J6300 Services Router**




## *Connecting DC Power*

**CAUTION:** If your J6300 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 86.

To connect DC power to the router:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis. For more information about ESD, see “Preventing Electrostatic Discharge Damage” on page 195.
2. Use a grounding cable to connect the router to earth ground: (For cable requirements, see “Chassis Grounding” on page 96.)

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 screw and washer from the PEM nut 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 47 on page 100, Figure 48 on page 101, and Figure 49 on page 101.

e. Secure the cable lug to the grounding point, first with the washer, then with the screw.

---

**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:** You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. 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.

---

   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 47: Connecting DC Power to the J2300 Services Router**

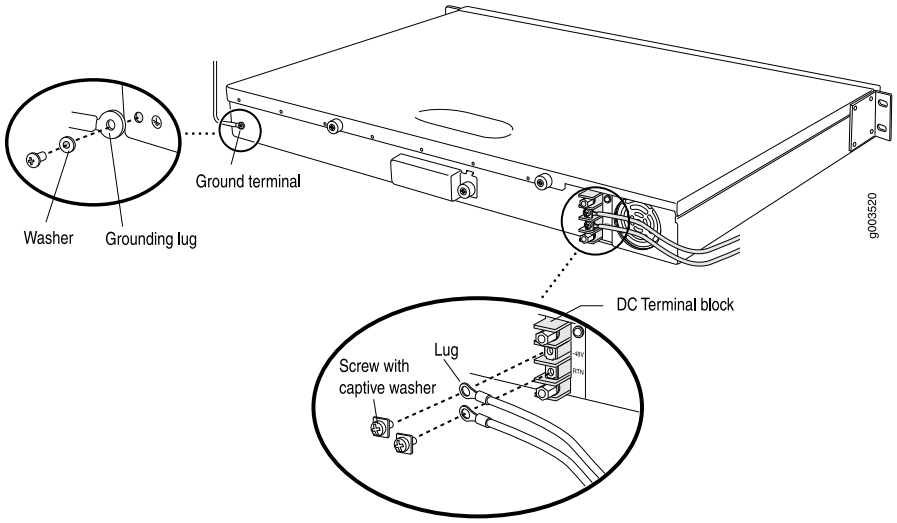


**Figure 48: Connecting DC Power to the J4300 Services Router**

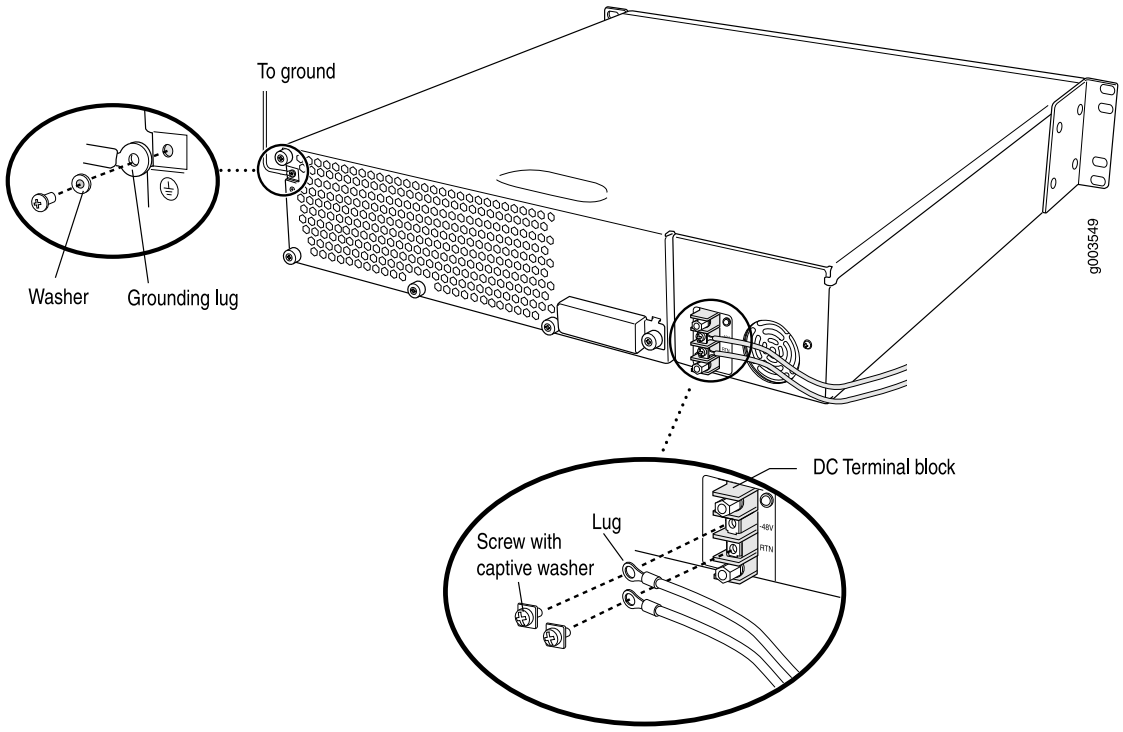
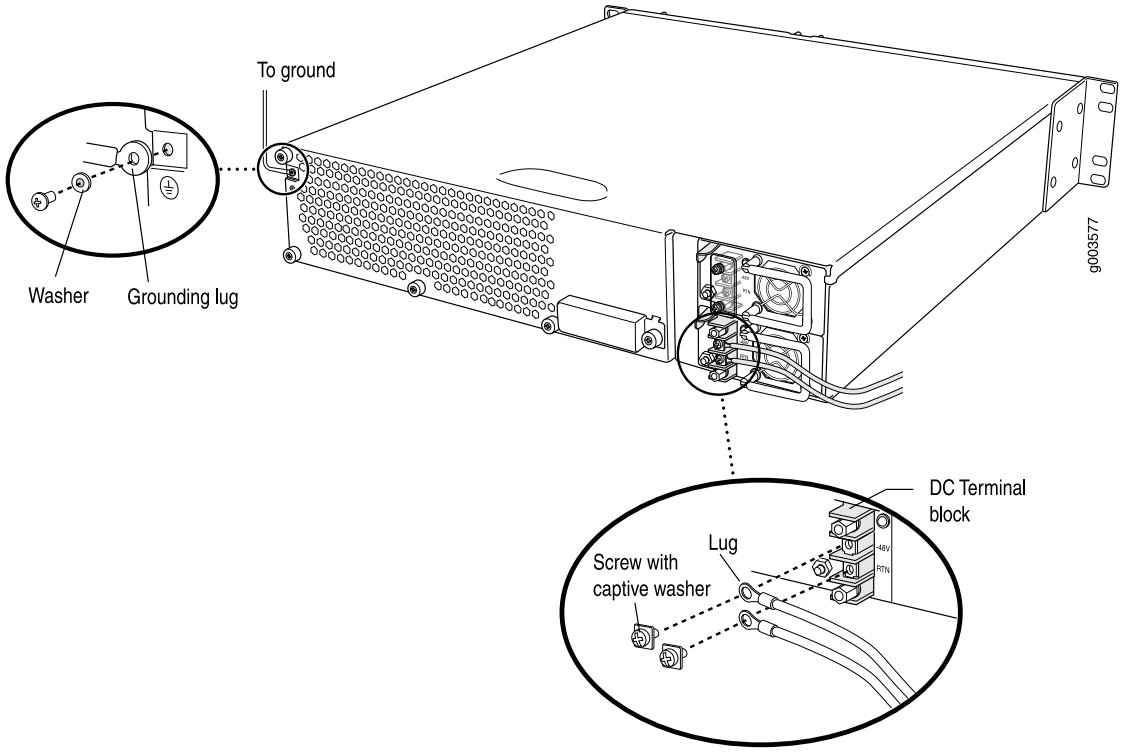



**Figure 49: Connecting DC Power to the J6300 Services Router**



## 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 61.

If you are setting up many Services Routers, autoinstallation can help automate the configuration process. For more information about autoinstallation, see the *J-series Services Router Administration Guide*.

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



## Basic Connectivity Terms

Before configuring basic connectivity, become familiar with the terms defined in Table 45 on page 103.

**Table 45: Basic Connectivity Terms**

| Term | Definition |
|---|---|
| **domain name** | Name that identifies the network or subnetwork of a router. |

**Table 45: Basic Connectivity Terms** *(continued)*

| Term | Definition |
|---|---|
| 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*

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 Fast Ethernet interfaces, fe-0/0/0 and fe-0/0/1, 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 fe-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 fe-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 fe-0/0/0 to 192.168.1.1/24 and becomes a DHCP server out the fe-0/0/0 interface.

**NOTE:** If the fe-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 fe-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 fe-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 89.
- 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 fe-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 109
- Connecting to the CLI Locally on page 111
- Connecting to the CLI Remotely on page 113


### *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 50 on page 110 and Figure 51 on page 111.

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 50 on page 110 and Figure 51 on page 111):

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 115.

**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 50: Connecting to the Fast Ethernet Port on the J2300 Services Router**

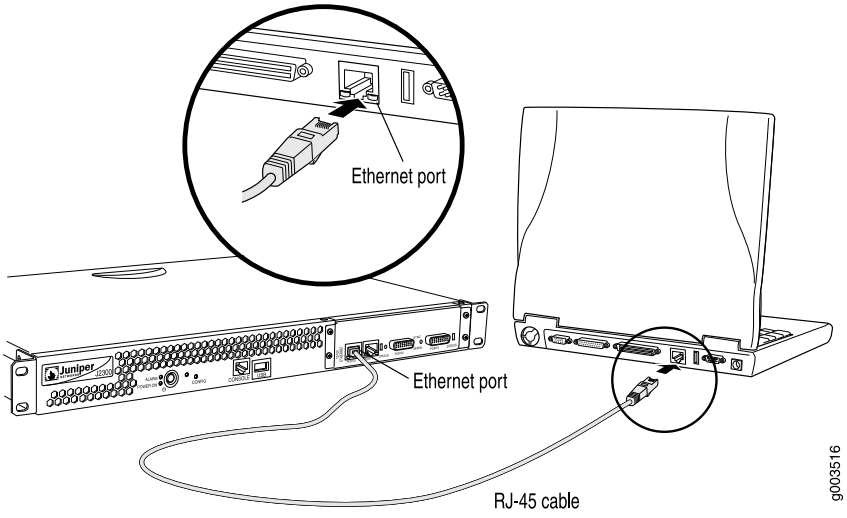
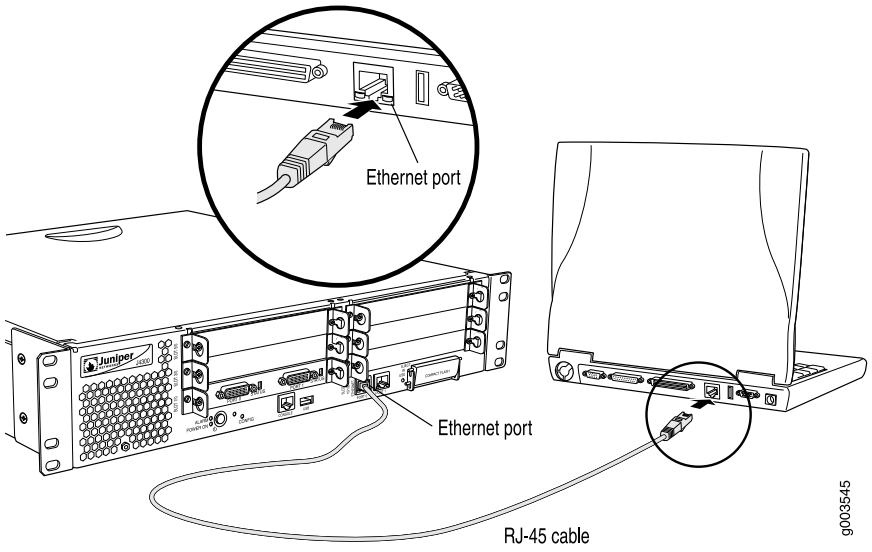


**Figure 51: Connecting to the Fast Ethernet Port on the J4300 or J6300 Services Router**




## *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 52 on page 112 and Figure 53 on page 113.

---

**NOTE:** Figure 52 on page 112 and Figure 53 on page 113 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 cable supplied with your router into the RJ-45 to DB-9 serial port adapter supplied with your router (see Figure 52 on page 112 and Figure 53 on page 113).
4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see Figure 52 on page 112 and Figure 53 on page 113).
5. Connect the other end of the Ethernet cable to the console port on the router (Figure 52 on page 112 and Figure 53 on page 113).
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 52: Connecting to the Console Port on the J2300 Services Router**

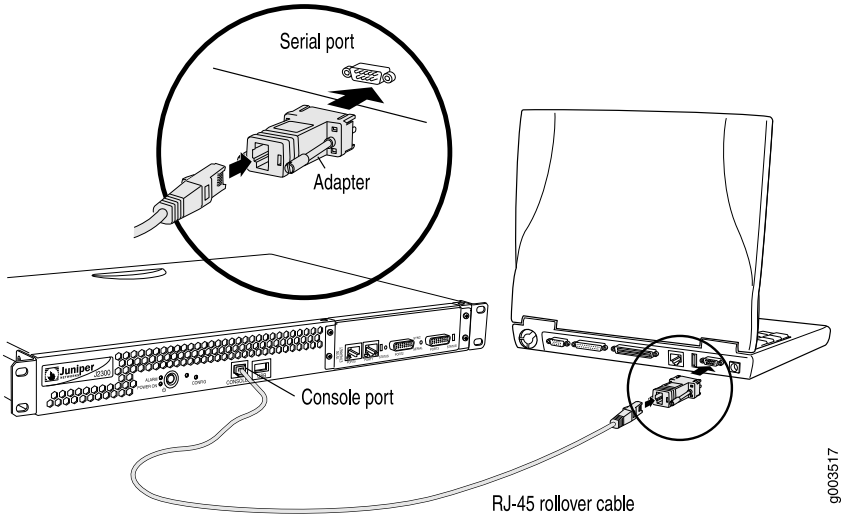
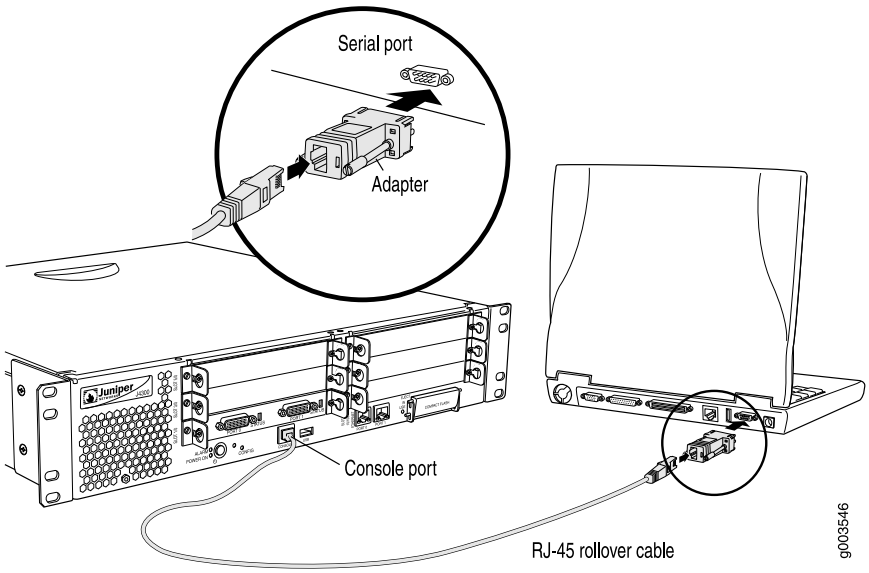


**Figure 53: Connecting to the Console Port on the J4300 or J6300 Services Router**




## *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

**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 cable supplied with your router into the console port on the router.
4. Plug the other end of the Ethernet 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 36 on page 65 shows the Quick Configuration page for basic setup.

Before you configure the router, gather the information described in "Before You Begin" on page 108.

To configure basic settings with J-Web Quick Configuration:

1. If you have not already done so, connect a management device to the fe-0/0/0 interface on port 0. For instructions, see "Connecting to the J-Web Interface" on page 109.
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 46 on page 116.

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 fe-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 fe-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 121.

**Table 46: 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.<br>**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**.<br>To delete an IP address, click on it in the box above the Add button, then click **Delete**. |

**Table 46: 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.<br><br>**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**.<br><br>■ 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**.<br><br>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**.<br><br>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. |
| fe-0/0/0 Address | Defines the IP address and prefix length of fe-0/0/0. The interface fe-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.<br><br>**NOTE:** You must enter the fe-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. |
| 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 47 on page 118. Determine the values to set on the Services Router in your network.

**Table 47: 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 fe-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 fe-0/0/0 interface on port 0. For instructions, see "Connecting to the J-Web Interface" on page 109. You can also connect to the CLI to configure basic settings. For instructions, see "Connecting to the CLI Locally" on page 111 and "Connecting to the CLI Remotely" on page 113.

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 48 on page 119.

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 121.

**Table 48: 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**.<br>2. Next to System, click **Configure** or **Edit**. | From the [edit] hierarchy level, enter<br>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:<br>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:<br>set domain-name lab.router.net |
| Allow SSH remote access. | 1. In the Nested configuration section, next to Services, click **Configure** or **Edit**.<br>2. Next to Ssh, click **Configure** or **Edit**.<br>3. Click **OK**.<br>4. Click **OK** a second time to return to the System level in the configuration editor hierarchy. | Set remote access for SSH:<br>set services ssh |
| Define root authentication for access to the router.<br>**NOTE:** For readability, the entire key is not shown. | 1. In the Nested configuration section, next to Root authentication, click **Configure** or **Edit**.<br>2. Next to Ssh rsa, click **Add New Entry**.<br>3. In the Authorized key box, type the RSA password—for example, ssh-rsa AAAAB3Nza...D9Y2gXF9ac== root@routera.lab.router.net<br>4. Click **OK**.<br>5. Click **OK** a second time to return to the System level in the configuration editor hierarchy. | Set the root password. For example:<br>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:<br>set time-zone America/Los_Angeles |

**Table 48: Configuring Basic Settings** *(continued)*

| Task | J-Web Configuration Editor | CLI Configuration Editor |
|---|---|---|
| Define the NTP server that NTP requests can be sent to. | 1. In the Nested configuration section, next to Ntp, click **Configure** or **Edit**.<br>2. Next to Server, click **Add New Entry**.<br>3. In the Address box, type the NTP server's IP address—for example, 10.148.2.21<br>4. Click **OK**.<br>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:<br>set ntp server 10.148.2.21 |
| Define the DNS server that receives DNS requests. | 1. Next to Name server, click **Add New Entry**.<br>2. In the Address box, type the address of the DNS server—for example, 10.148.2.32.<br>3. Click **OK**. | Set the address of the DNS server. For example:<br>set name-server 10.148.2.32 |
| Add each domain that the router belongs to. | 1. Next to Domain search, click **Add New Entry**.<br>2. In the Value box, type the name of the domain in which the router is located—for example, lab.router.net.<br>3. Click **OK**.<br>4. Next to Domain search, click **Add New Entry**.<br>5. In the Value box, type the name of another domain that the router belongs to—for example, router.net.<br>6. Click **OK**. | Set the domains to be searched. For example:<br>set domain-search lab.router.net<br>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:<br>set backup router address 192.168.2.44 |
| Define the IP address for lo0.0. | 1. In the configuration editor hierarchy, next to Interfaces, click **Configure** or **Edit**.<br>2. In the Interface table, locate the lo0 row and click **Unit**.<br>3. In the Unit table, click **0**, and in the Family section next to Inet, click **Configure** or **Edit**.<br>4. To delete the existing IP address, click the **Discard** button. Select the **Delete Configuration Below This Point** option button from the next display.<br>5. Next to Address, click **Add new entry**.<br>6. In the Source box, type the address and prefix length for the loopback interface—for example, 172.16.1.24/32.<br>7. Click **OK**. | 1. From the [edit] hierarchy level, enter<br>edit interfaces<br>2. Delete the existing IP address:<br>delete lo0 unit 0 family inet address<br>3. Set the IP address and prefix length of lo0.0. For example:<br>set lo0 unit 0 family inet address 172.16.1.24/32 |

**Table 48: Configuring Basic Settings** *(continued)*

| Task | J-Web Configuration Editor | CLI Configuration Editor |
|---|---|---|
| Define the IP address for fe-0/0/0. | 1. In the configuration editor hierarchy, next to Interfaces, click **Configure** or **Edit**.<br>2. In the Interface table, locate the fe-0/0/0 row and click **Unit**.<br>3. In the Unit table, click **0**, and in the Family section next to Inet, click **Configure** or **Edit**.<br>4. To delete the existing IP address, click the **Discard** button. Select the **Delete Configuration Below This Point** option button from the next display.<br>5. Next to Address, click **Add new entry**.<br>6. In the Source box, type the address and prefix length for the management interface—for example, 192.168.1.1/24.<br>7. Click **OK**. | 1. Delete the existing IP address:<br>delete fe-0/0/0 unit 0 family inet address.<br>2. Set the IP address and prefix length of fe-0/0/0. For example:<br>set fe-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 48 on page 119. Your output displays the values you set.

```
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 {
    fe-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

Before configuring secure Web access, become familiar with the terms defined in Table 49 on page 123.

**Table 49: 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 49: 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 103.

- Obtain an SSL certificate from a trusted signing authority. See “Generating SSL Certificates” on page 125.

### *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.

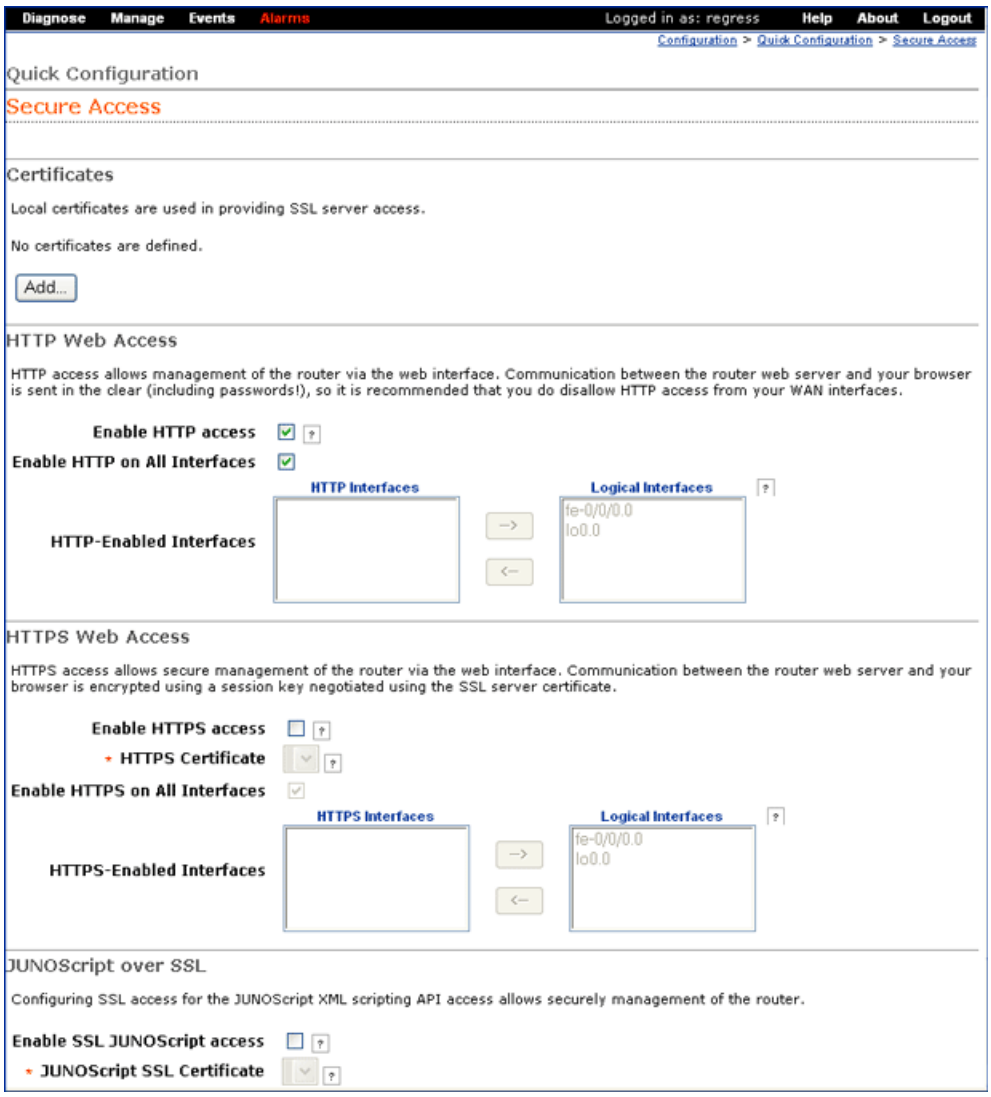
You can use either J-Web Quick Configuration or a configuration editor to install the SSL certificate and enable HTTPS.

## Configuring Secure Web Access

Navigate to the Secure Access Quick Configuration page by selecting **Configuration > Quick Configuration > Secure Access**. On this page, you can enable HTTP and HTTPS access on interfaces for managing Services Routers through the Web interface. You can also install SSL certificates and enable JUNOScript over SSL with the Secure Access page.

Figure 54 on page 126 shows the Secure Access Quick Configuration page.

**Figure 54: Quick Configuration Secure Access Page**




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

1. Enter information into the Secure Access Quick Configuration page, as described in Table 50 on page 127.
2. 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**.

3. To verify that Web access is enabled correctly, connect to the routing platform 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*.
4. To verify the secure Web access configuration, see "Verifying Secure Web Access" on page 129.

**Table 50: Secure Access Quick Configuration Summary**

| Field | Function | Your Action |
|---|---|---|
| **Certificates** | | |
| Certificates | Displays digital certificates required for SSL access to the Services Router.<br><br>Allows you to add and delete SSL certificates.<br><br>For information about how to generate an SSL certificate, see "Generating SSL Certificates" on page 125. | To add a certificate:<br>1. Click **Add**. Opens the Add a Local Certificate page.<br>2. Type a name in the Certificate Name box—for example, new.<br>3. Paste the generated certificate and RSA private key in the Certificate box.<br><br>To delete a certificate, select it and click **Delete**. |
| **HTTP Web Access** | | |
| Enable HTTP Access | Enables HTTP access on interfaces. | To enable HTTP access, select the **Enable HTTP access** check box. |
| Enable HTTP on All Interfaces | Enables HTTP access on all interfaces at one time. | To enable HTTP access on all interfaces, select the **Enable HTTP on All Interfaces** check box. |
| HTTP-Enabled Interfaces | Specifies interfaces on which you want to enable HTTP access. | Select and deselect interfaces by clicking the direction arrows:<br>■ To enable HTTP access on an interface, add the interface to the HTTP Interfaces list.<br>■ 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.<br><br>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**. |

**Table 50: Secure Access Quick Configuration Summary** *(continued)*

| Field | Function | Your Action |
|---|---|---|
| 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. |
| 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:<br>■ To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list.<br>■ 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.<br><br>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 51 on page 128.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see "Verifying Secure Web Access" on page 129.

**Table 51: 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 > View and Edit > Edit Configuration**.<br>2. Next to Security, click **Configure** or **Edit**. | From the [edit] hierarchy level, enter<br><br>edit security |

**Table 51: 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.<br><br>For information about generating SSL certificates, see "Generating SSL Certificates" on page 125. | 1. Next to Certificates, click **Configure**.<br>2. Next to Local, click **Add new entry**.<br>3. In the Name box, type a name for the certificate to be imported—for example, new.<br>4. In the Certificate box, paste the generated SSL certificate and private key.<br>5. Click **OK**. | Enter<br><br>set certificates local new load-key-file*path*<br><br>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.<br><br>Specify the port on which HTTPS access is to be enabled—for example, TCP port 8443.<br><br>**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**.<br>2. Select the **Services** check box and click **Edit** next to it.<br>3. Next to Web management, click **Edit**.<br>4. Select the **Https** check box and click **Edit** next to it.<br>5. In the Local certificate box, type the name of the certificate—for example, new.<br>6. In the Port box, type 8443.<br>7. Click **OK**. | From the [edit system] hierarchy level, enter<br><br>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 129
- Displaying a Secure Access Configuration on page 130

### *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 125.

```
[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 51 on page 128.

```
[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

# 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

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*

Each feature license is tied to exactly one software feature, and that license is valid for exactly one Services Router. Table 52 on page 131 lists the Services Router software features that require licenses.

**Table 52: J-series Services Router Software Feature Licenses**

| Licensed Software Feature | License Name |
|---|---|
| **IBM Networking** | |

**Table 52: J-series Services Router Software Feature Licenses** *(continued)*

| Licensed Software Feature | License Name |
|---|---|
| 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 103.

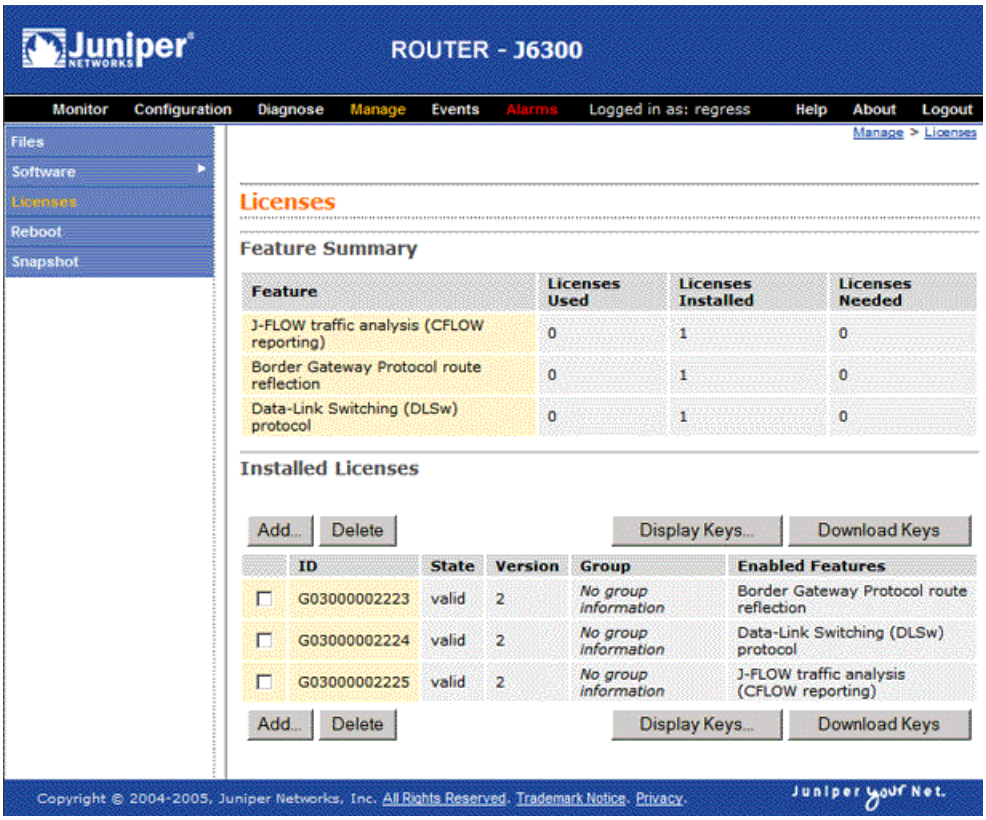
## Managing J-series Licenses with the J-Web Interface

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 55 on page 133 shows the J-Web Licenses page.

**Figure 55: 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 53 on page 133.

**Table 53: Summary of License Management Fields**

| Field Name | Definition |
|---|---|
| **Feature Summary** | |

**Table 53: Summary of License Management Fields** *(continued)*

| Field Name | Definition |
|---|---|
| Feature | Name of the licensed feature:<br>■ J-series licenses listed in Table 52 on page 131.<br>■ 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.<br>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.<br>If the license requires a group license, this field displays the required group definition.<br>**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*

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 138


### *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.

```
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.

```
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.

```
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

Chapter 10

# 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 167.

This chapter contains the following topics:



## Replacing Hardware Components

This section contains the following topics:



### *Tools and Parts Required*

To replace hardware components, you need the tools and parts listed in Table 54 on page 144.

**Table 54: 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<br>■ DRAM modules<br>■ 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 175.

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 52 on page 112 and Figure 53 on page 113).
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:

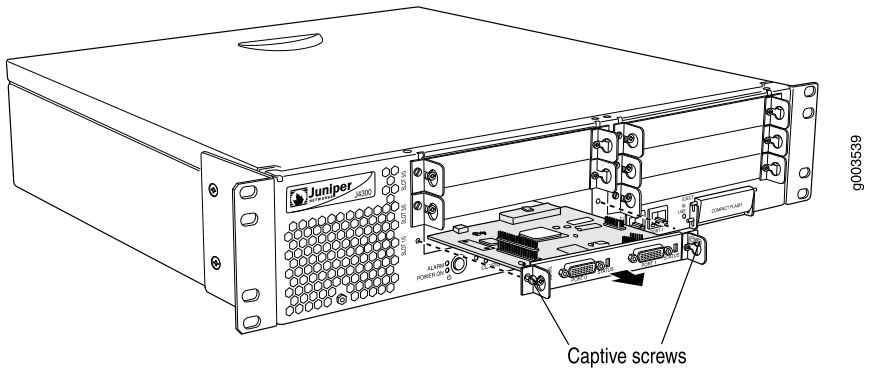


### Removing a PIM

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.

**Figure 56: Removing a PIM**



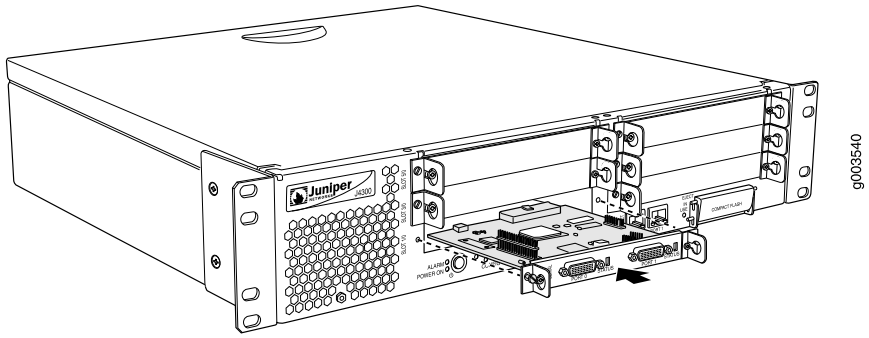

To remove a PIM (see Figure 56 on page 145):

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 195.
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.

## 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.

**Figure 57: Installing a PIM**




To install a PIM (see Figure 57 on page 146):

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 195.
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 47.

   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.

9. Complete the initial configuration of each network interface by using the CLI or J-Web interface. For information about configuring network interfaces, see the *J-series Services Router Basic LAN and WAN Access Configuration Guide*.

## *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 147
- 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 175.
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.

## *Removing and Installing the Primary Compact Flash Disk*

The primary compact flash drive is located in a slot at the rear of the Services Router as shown in Figure 2 on page 12, Figure 8 on page 22, and Figure 10 on page 22. The primary compact flash disk provides primary storage for the router. It can accommodate software images, configuration files, and microcode.

For information about configuring the primary compact flash disk, see the *J-series Services Router Administration Guide*.

To remove and install a primary compact flash disk, perform the following procedures:

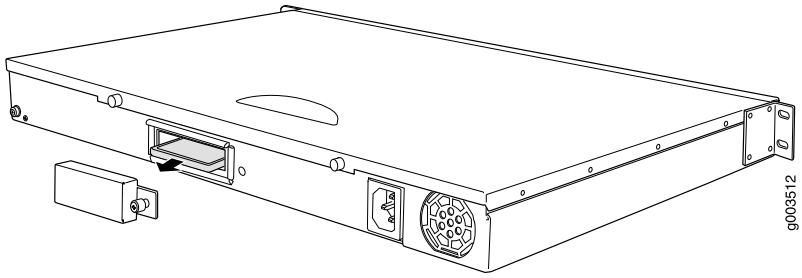
- Removing the Primary Compact Flash Disk on page 149
- Installing the Primary Compact Flash Disk on page 149

## Removing the Primary Compact Flash Disk

To remove the primary compact flash disk (see Figure 58 on page 149):

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 model.
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 from the power supply.
5. Loosen the thumbscrew that secures the primary compact flash drive cover on the rear of the chassis.
6. Remove the compact flash drive cover.
7. Gently grasp the compact flash disk, and slide it out of the connector (see Figure 58 on page 149).
8. Place the compact flash disk on the antistatic mat or in the electrostatic bag.

**Figure 58: Removing the Primary Compact Flash Disk**



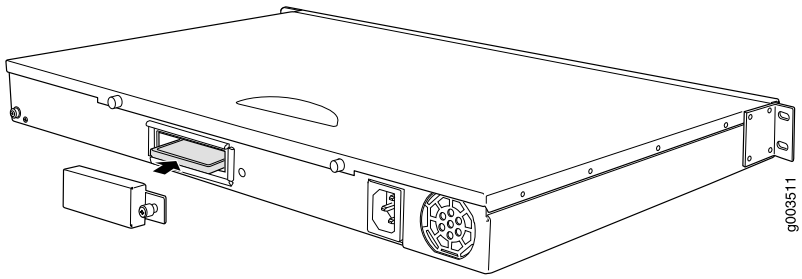

## Installing the Primary Compact Flash Disk

To install the primary compact flash disk (see Figure 59 on page 150):

**NOTE:** If you plan to boot the Services Router from the primary compact flash disk, you must first configure the primary compact flash disk in another router or with a computer running UNIX or Cygwin. For more information, see the *J-series Services Router Administration Guide*.

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 the Getting Started Guide for your model.
2. Press and release the power button to power off the router. Wait for the POWER LED to turn off.
3. Remove the power cord from the power supply.
4. Loosen the thumbscrew that secures the primary compact flash drive cover on the rear of the chassis.
5. Remove the compact flash drive cover.
6. Slide the compact flash disk into the connector on the Routing Engine (see Figure 59 on page 150).
7. Replace the compact flash drive cover.
8. Tighten the thumbscrew that secures the compact flash drive cover to the rear of the chassis.
9. Plug the power cord into the power supply.
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.

**Figure 59: Installing the Primary Compact Flash Disk**




## *Removing and Installing the Removable Compact Flash Disk*

The removable compact flash disk is an optional component on J4300 and J6300 Services Routers. The removable compact flash disk provides secondary storage for the router. It can accommodate software images, configuration files, and microcode. If the primary compact flash disk fails on startup, the router boots from the removable compact flash disk.

For information about configuring the removable compact flash disk, see the *J-series Services Router Administration Guide*.

To remove and install a removable compact flash disk, perform the following procedures:

- Removing the Removable Compact Flash Disk on page 151
- Installing the Removable Compact Flash Disk on page 152

### Removing the Removable Compact Flash Disk

**NOTE:** Depending on your configuration, the Services Router might not have a backup compact flash drive. If no backup compact flash drive is installed, proceed directly to the next section, "Installing the Removable Compact Flash Disk" on page 152.

The removable compact flash drive is located in a slot on the front panel of the Services Router. To remove the removable compact flash disk (see Figure 60 on page 152):

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 195.
3. Verify the CF REMOVE LED is off.

   If the CF REMOVE LED is on, the router might have booted from the removable compact flash disk.

   To see which device the router used to boot, issue the show system storage command from the CLI. For example:

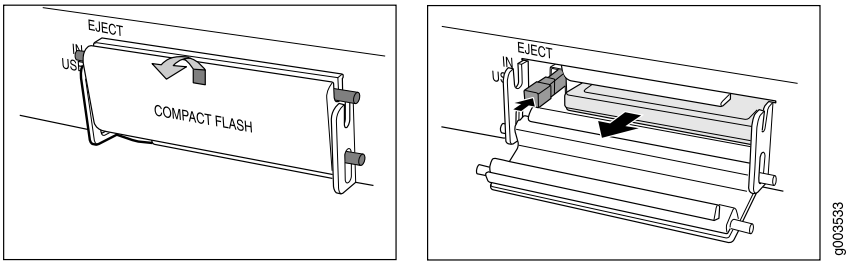
   ```
   user@host> show system storage

   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 *removable* compact flash disk is located at ad2. The USB storage device is located at usb0. 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 removable compact flash disk, press and release the power button to power off the router. Wait for the POWER LED to turn off before you remove the compact flash drive.
5. Slide the compact flash drive door up to unlatch the door, then tilt the top of the door out (see Figure 60 on page 152).

6. Eject the removable compact flash disk by pressing the button to the left of the compact flash drive once to unlock the button, and again to eject the compact flash drive.
7. Gently grasp the compact flash disk, and slide it out of the connector.
8. Place the compact flash disk on the antistatic mat or in the electrostatic bag.

**Figure 60: Removing the Removable Compact Flash Disk**

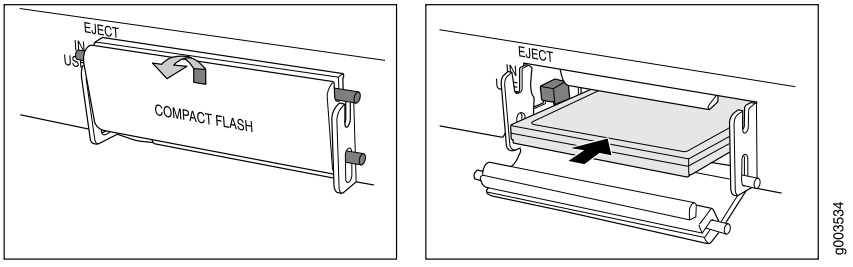



## Installing the Removable Compact Flash Disk

To install the removable compact flash disk, follow this procedure (see Figure 61 on page 152):

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 195.
2. Slide the compact flash door up to unlatch the door, then tilt the top of the door out (see Figure 61 on page 152).
3. Slide the compact flash disk into the connector on the Routing Engine.
4. Tilt the compact flash door in, and slide it down until it is secured.
5. To configure the removable compact flash disk with the request system snapshot command, see the *J-series Services Router Administration Guide*.

**Figure 61: Installing the Removable Compact Flash Disk**



## *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 153
- Installing the USB Storage Device on page 154

### 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 154.

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 195.
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 removable compact flash disk is located at ad2. 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 195.
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 62 on page 155 and Figure 63 on page 155.

**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 transfer a DRAM module between a J4300 and a J6300 Services Router, but not between these models and any other Services Router.

**Figure 62: J2300 DRAM Location**

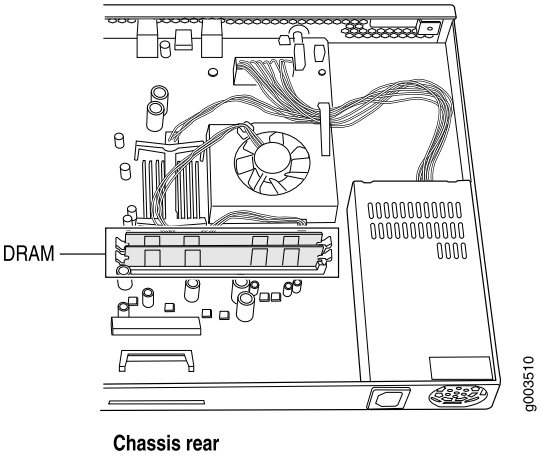
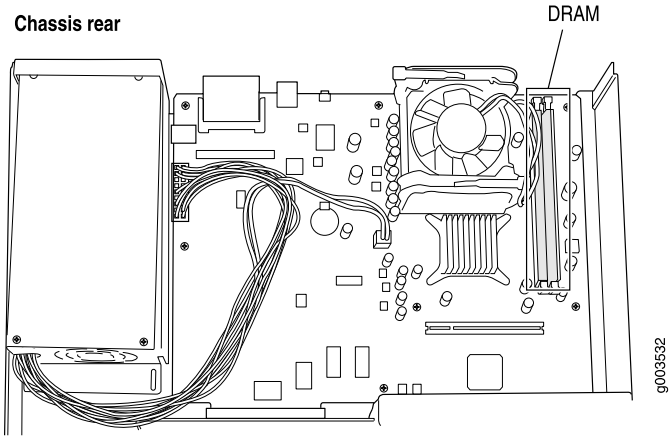



**Figure 63: J4300 and J6300 DRAM Location**




To modify the DRAM configuration, use the following procedures:

- Removing a DRAM Module on page 155
- 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 64 on page 156 or Figure 65 on page 157).
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 64: Adding or Replacing a DRAM Module in a J2300 Chassis**

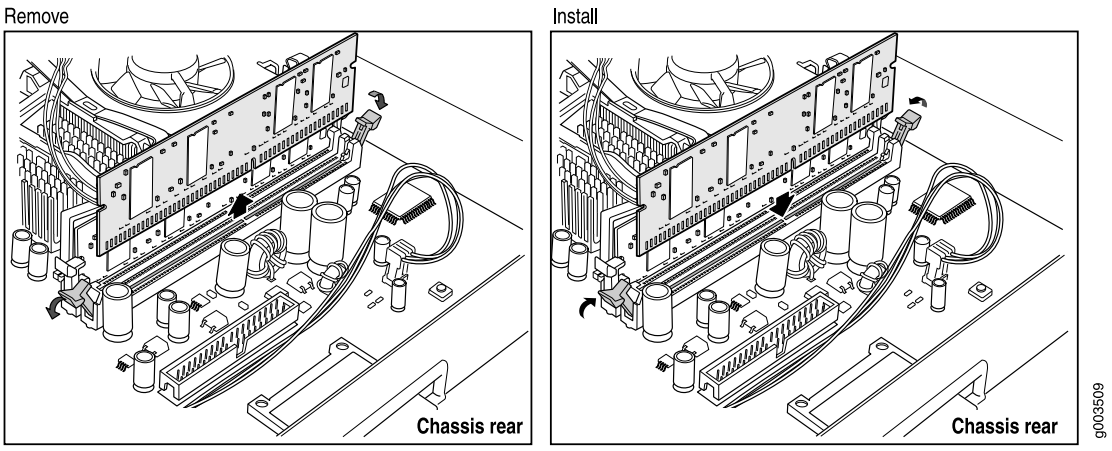
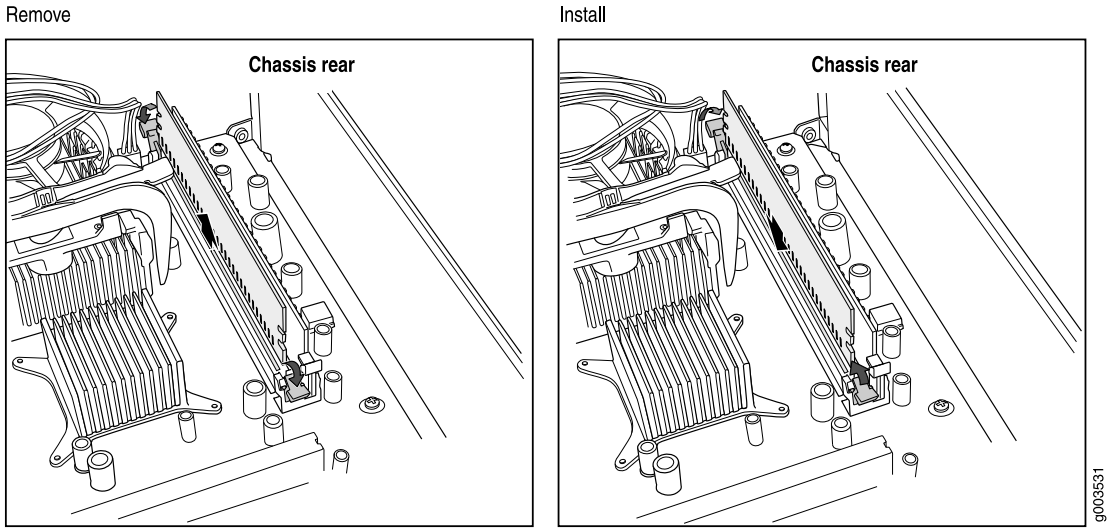


**Figure 65: Adding or Replacing a DRAM Module in a J4300 or J6300 Chassis**




## Installing a DRAM Module

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 64 on page 156 or Figure 65 on page 157).
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 64 on page 156 or Figure 65 on page 157).
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 add a second power supply to the J6300 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 10 on page 22 or Figure 11 on page 23). Each J6300 power supply provides power to all components in the router. The J6300 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 J6300 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 158
- Removing an AC Power Supply from a J6300 Router on page 159
- Installing an AC Power Supply in a J6300 Router on page 160
- Replacing a DC Power Supply Cable on page 161
- Removing a DC Power Supply on page 162
- Installing a DC Power Supply on page 163

### 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 85).
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 195.

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 J6300 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 96.

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 J6300 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 J6300 Services Router (see Figure 66 on page 160):

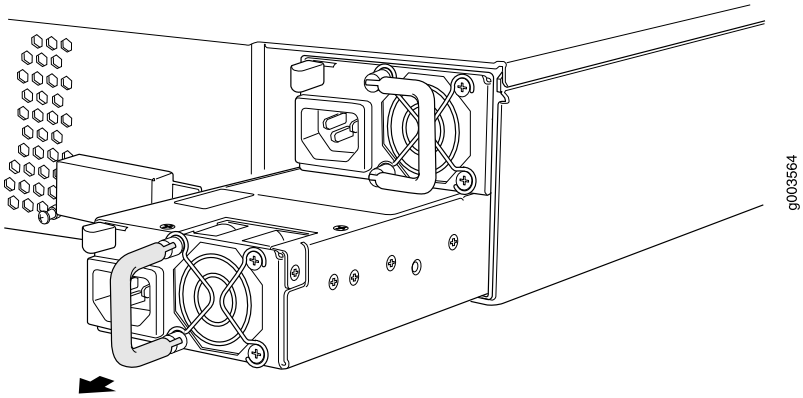
1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 195.
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 J6300 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 66 on page 160).
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 66: Removing an AC Power Supply**




## Installing an AC Power Supply in a J6300 Router

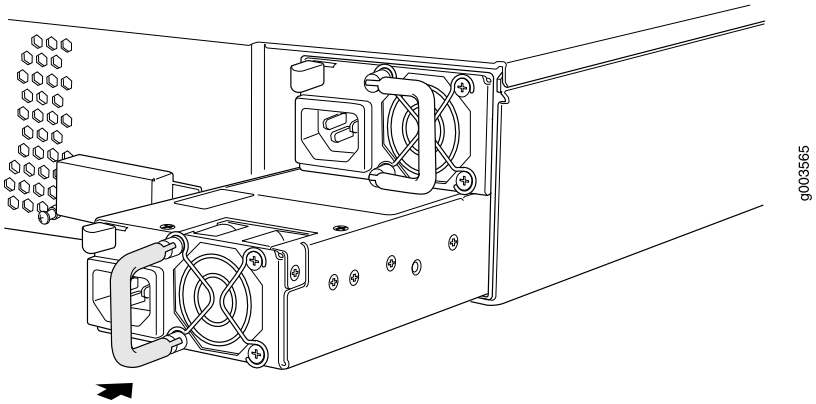
To install an AC power supply in a J6300 Services Router (see Figure 67 on page 161):

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 195.
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 96.

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 67: 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 96 and "DC Power, Connection, and Power Cable Specifications" on page 86.

**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 195.
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:** You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. 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.

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 96.

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

The power supplies are located at the right rear of the chassis. A power supply weighs 2.4 lb (1.1 kg).

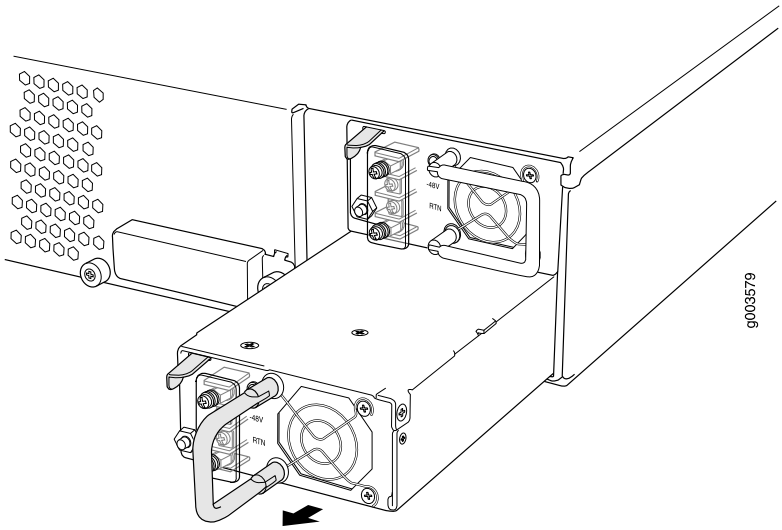
To remove a DC power supply (see Figure 68 on page 163):

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 195.
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:** You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. 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.

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 68 on page 163).
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 68: Removing a DC Power Supply**




## Installing a DC Power Supply

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 (see Figure 69 on page 165):

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:** You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. 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.

---

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 195.
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.

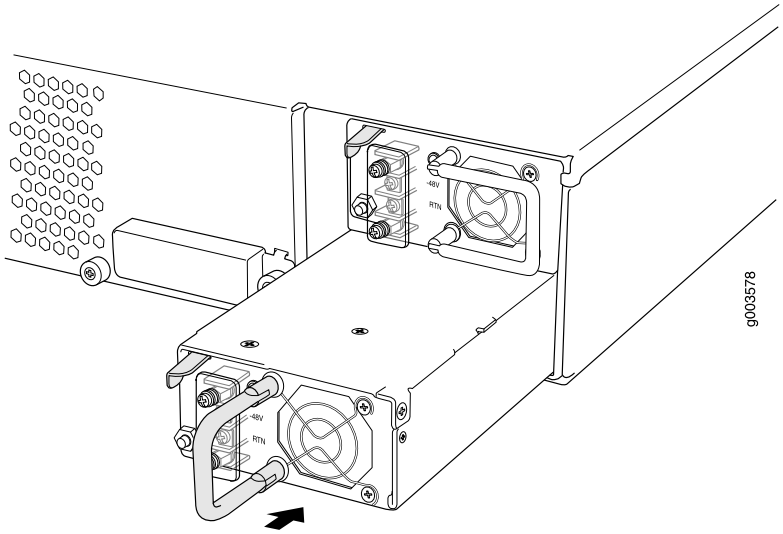
---

**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 96.

---

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 69: Installing a DC Power Supply**




## 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 165
- Contacting the Juniper Networks Technical Assistance Center on page 166

### *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.

**NOTE:** The ALARM LED on the Services Router lights yellow whether the alarm condition is major (red) or minor (yellow).

To view a more detailed description of the alarm cause, issue the show chassis alarms CLI command:

```
user@host> show chassis alarms
```

Table 55 on page 166 describes alarms that can occur for a chassis component such as the Routing Engine or a Physical Interface Module (PIM).

**Table 55: 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.<br><br>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.<br><br>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) |
| 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*.)<br><br>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 81.)<br>■ Check the air flow. (See "General Site Guidelines" on page 79.)<br>■ Check the fans. (See "J2300 Cooling System" on page 19 or "J4300 and J6300 Cooling System" on page 30.) If you must replace a fan or the Routing Engine, contact JTAC. (See "Requesting Support" on page xx.) | Yellow (minor) |
| | 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 11

# Contacting Customer Support and Returning Hardware

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



## Locating Component Serial Numbers

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

```
user@host> show chassis hardware
  Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                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 70 on page 168 through Figure 72 on page 169) attached to the component body.

**Figure 70: J2300 Serial Number ID Label**

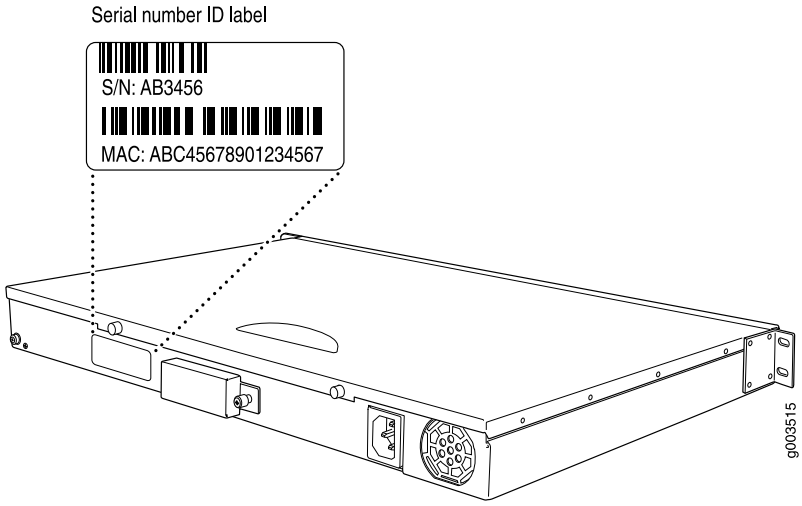



**Figure 71: J4300 Serial Number ID Label**

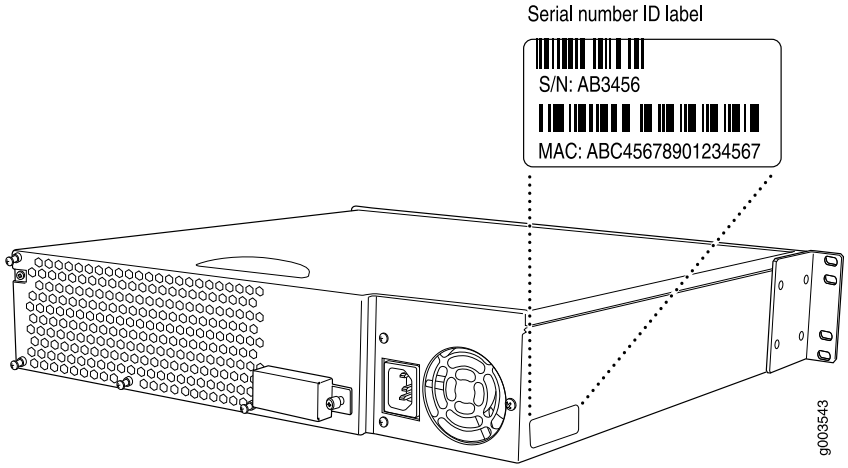
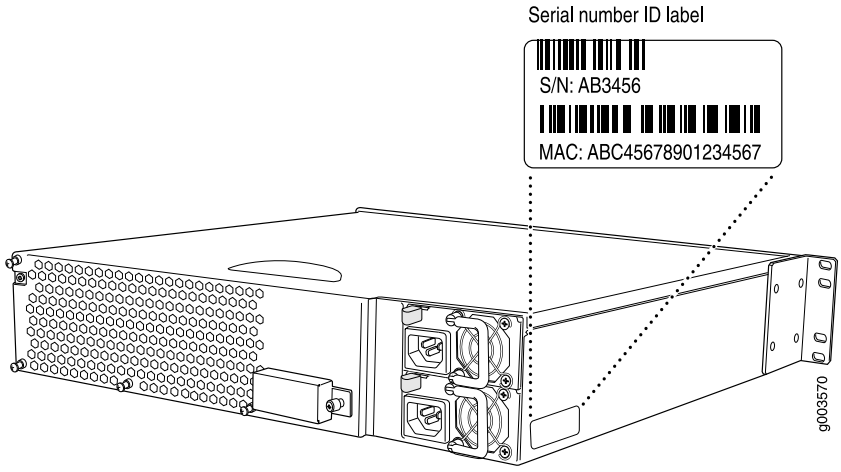


**Figure 72: J6300 Serial Number ID Label**




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

- PIM Serial Number Label on page 169
- J6300 Power Supply Serial Number Labels on page 169

### *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.

### *J6300 Power Supply Serial Number Labels*

The power supplies installed in the J6300 Services Router are field-replaceable. Each power supply has a unique serial number. The serial number label is located on the top of the 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 167.
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 171.

## Packing a Router or Component for Shipment

This section contains the following topics:



### *Tools and Parts Required*

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

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

### *Packing the Services Router for Shipment*

To pack the router for shipment, follow this procedure:

1. Retrieve the shipping carton and packing materials in which the router was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis, or to an outside ESD point if the router is disconnected from earth ground. For more information about ESD, see "Preventing Electrostatic Discharge Damage" on page 195.
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 158.
6. Remove the cables that connect to all external devices. For instructions, see “Removing a PIM Cable” on page 147.
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

Chapter 12

# Network Cable Specifications and Connector Pinouts

The network interfaces supported on the router accept different kinds of network cable.



## Serial PIM Cable Specifications

The 2-port serial PIM uses the cables and connectors summarized in Table 56 on page 175. Pinouts are detailed in Table 57 on page 176 through Table 66 on page 184.

**Table 56: 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 57 on page 176 |
| RS-232 DCE | DB-25 female | 4-40 threaded jacknuts | 13 | Table 58 on page 177 |
| RS-422/449 (EIA-449) DTE | DC-37 (DB-37) male | 4-40 threaded jackscrews | 25 | Table 59 on page 177 |
| RS-422/449 (EIA-449) DCE | DC-37 (DB-37) female | 4-40 threaded jacknuts | 25 | Table 60 on page 178 |
| EIA-530A DTE | DB-25 male | 4-40 threaded jackscrews | 23 | Table 61 on page 180 |

**Table 56: 2-Port Serial PIM Cables and Connectors** *(continued)*

| Name | Connector | Connector Hardware | End-to-End Conductors | Pinouts |
|---|---|---|---|---|
| EIA-530A DCE | DB-25 female | 4-40 threaded jacknuts | 22 | Table 62 on page 181 |
| V.35 DTE | M/34 male | Standard (Normally included with M/34 connector shell) | 18 | Table 63 on page 182 |
| V.35 DCE | M/34 female | Standard (Normally included with M/34 connector shell) | 18 | Table 64 on page 183 |
| X.21 DTE | DB-15 male | M3 threaded jackscrews | 13 | Table 65 on page 183 |
| X.21 DCE | DB-15 female | M3 threaded jacknuts | 13 | Table 66 on page 184 |

## *RS-232 DTE Cable Pinout*

**Table 57: 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 |
| 22 to 21 | – | – | – |
| 18 to 17 | – | – | – |

## *RS-232 DCE Cable Pinout*

**Table 58: 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 59: 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) |
| 37 | 9 | 38 | Clear to Send (A) |

**Table 59: RS-422/449 (EIA-449) DTE Cable Pinout** *(continued)*

| LFH-60 Pin | DC-37 (DB-37) Pin | LFH-60 Pairing | Description |
|---|---|---|---|
| 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 60: 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) |

**Table 60: RS-422/449 (EIA-449) DCE Cable Pinout** *(continued)*

| LFH-60 Pin | DC-37 (DB-37) Pin | LFH-60 Pairing | Description |
|---|---|---|---|
| 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 |
| 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 61: 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) |
| 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 62: 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) |
| 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 63: 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) |
| 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 64: 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) |
| 22 to 21 | – | – | – |
| 26 to 25 | – | – | – |

## *X.21 DTE Cable Pinout*

**Table 65: X.21 DTE Cable Pinout**

| LFH-60 Pin | DB-15 Pin | LFH-60 Pairing | Description |
|---|---|---|---|
| 15 | 1 | – | Shield Ground |

**Table 65: X.21 DTE Cable Pinout** *(continued)*

| LFH-60 Pin | DB-15 Pin | LFH-60 Pairing | Description |
|---|---|---|---|
| 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 66: 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) |
| 57 | 8 | – | Signal Ground |
| 2 | 9 | 1 | Transmit Data (B) |
| 38 | 10 | 37 | Control (B) |
| 59 | 11 | 60 | Receive (B) |

**Table 66: X.21 DCE Cable Pinout** *(continued)*

| LFH-60 Pin | DB-15 Pin | LFH-60 Pairing | Description |
|---|---|---|---|
| 47 | 12 | 48 | Indicate (B) |
| 51 | 13 | 52 | Signal Element Timing (B) |
| 30 to 29 | – | – | – |

## Fast Ethernet RJ-45 Connector Pinout

Table 67 on page 185 describes the Fast Ethernet RJ-45 connector pinout information.

**NOTE:** Either a straight-through or cross-over cable can be used to connect to the interface.

**Table 67: Fast Ethernet RJ-45 Connector Pinout**

| Pin | Signal |
|---|---|
| 1 | TX + |
| 2 | TX- |
| 3 | RX + |
| 4 | Termination network |
| 5 | Termination network |
| 6 | RX- |
| 7 | Termination network |
| 8 | Termination network |

## Chassis Console Port Pinouts

The console port on a J-series Services Router chassis has an RJ-45 connector. Table 68 on page 186 provides RJ-45 chassis 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 68: RJ-45 Chassis 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 |
| 7 | DSR Input | Data Set Ready |
| 8 | CTS Input | Clear to Send |

Table 69 on page 186 describes the DB-9 connector pinouts.

**Table 69: 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 70 on page 187 through Table 73 on page 188 describe the RJ-48 connector pinouts.

**Table 70: 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, + |
| 3 | 3 | Shield/Return/Ground |
| 6 | 6 | Shield/Return/Ground |
| 7 | No connect | No connect |
| 8 | No connect | No connect |

**Table 71: 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 72: 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 |
| 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 73: 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 |

**Table 73: RJ-48 Connector to DB-15 Connector (Crossover) Pinout** *(continued)*

| RJ-48 Pin (on T1/E1 PIM) (Data Numbering Form) | DB-15 Pin (Data Numbering Form) | Signal |
|---|---|---|
| 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 74 on page 189 describes the RJ-11 connector pinout.

**Table 74: 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 75 on page 190 describes the RJ-45 connector pinout.

**Table 75: 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 13

# 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

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*

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.

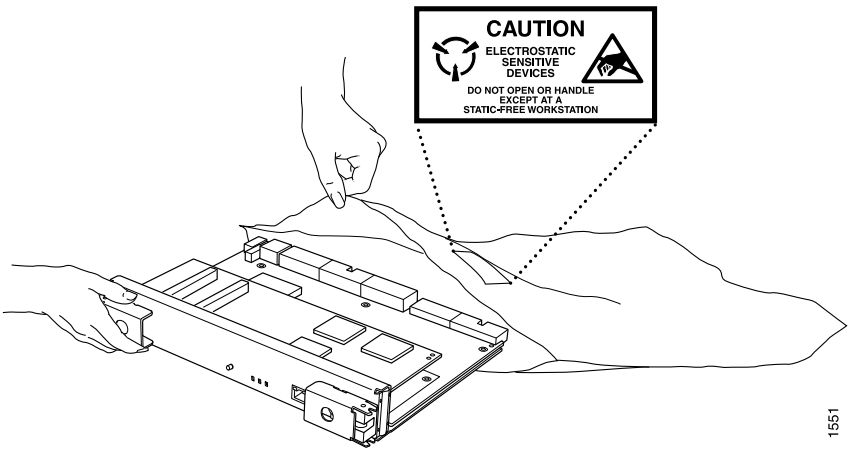
---

**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 8 on page 22 .
- 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 73 on page 196). If you are returning a component, place it in an electrostatic bag before packing it.

**Figure 73: 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

- 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 J6300 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.

### 冗余电源

如果 Juniper Networks 设备包含一个可选的冗余电源　请将两个电源连接到不同的输入电源。不这样做的结果是 Juniper Networks 设备一路供电出问题时导致全部的电源故障

### 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.

---

**WARNING: 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.

---

**WARNING: 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 96 and "DC Power, Connection, and Power Cable Specifications" on page 86.

**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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: ¡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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: 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.

**WARNING: ¡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.

**WARNING: 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 J6300 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 J6300 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 J6300 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 J6300 Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.

**WARNING: Avvertenza** Questa J6300 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 J6300 enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.

**WARNING: Aviso** Este J6300 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 J6300 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 J6300 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 210
- Installation Instructions Warning on page 210
- Rack-Mounting Requirements and Warnings on page 211
- Ramp Warning on page 215


### Chassis Lifting Guidelines

The weight of a fully populated chassis is approximately 12 lbs (5.4 kg) for a J2300 Services Router, 21 lbs (9.5 kg) for a J4300 Services Router, and 24 lb (10.9 kg) for a J6300 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 79 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

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 220
- Jewelry Removal Warning on page 221
- Lightning Activity Warning on page 222

### 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 227
- European Community on page 229
- Japan on page 231
- Taiwan on page 232
- United States on page 232


### *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.

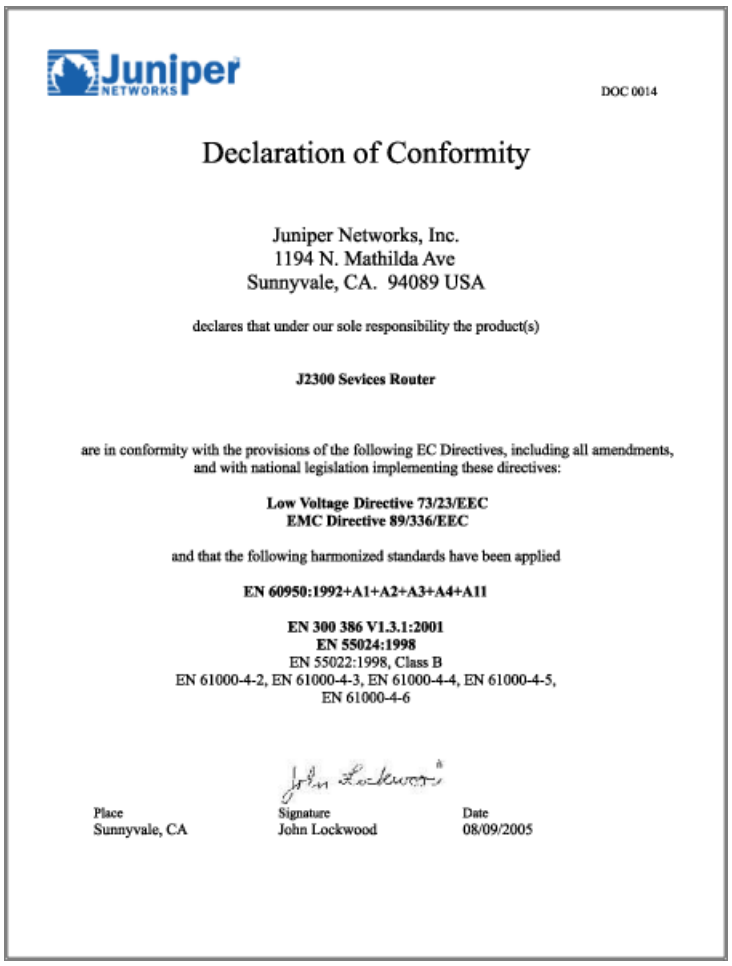
---

**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*



Juniper NETWORKS

DOC 0014

## Declaration of Conformity

Juniper Networks, Inc.
1194 N. Mathilda Ave
Sunnyvale, CA. 94089 USA

declares that under our sole responsibility the product(s)

**J2300 Sevices Router**

are in conformity with the provisions of the following EC Directives, including all amendments, and with national legislation implementing these directives:

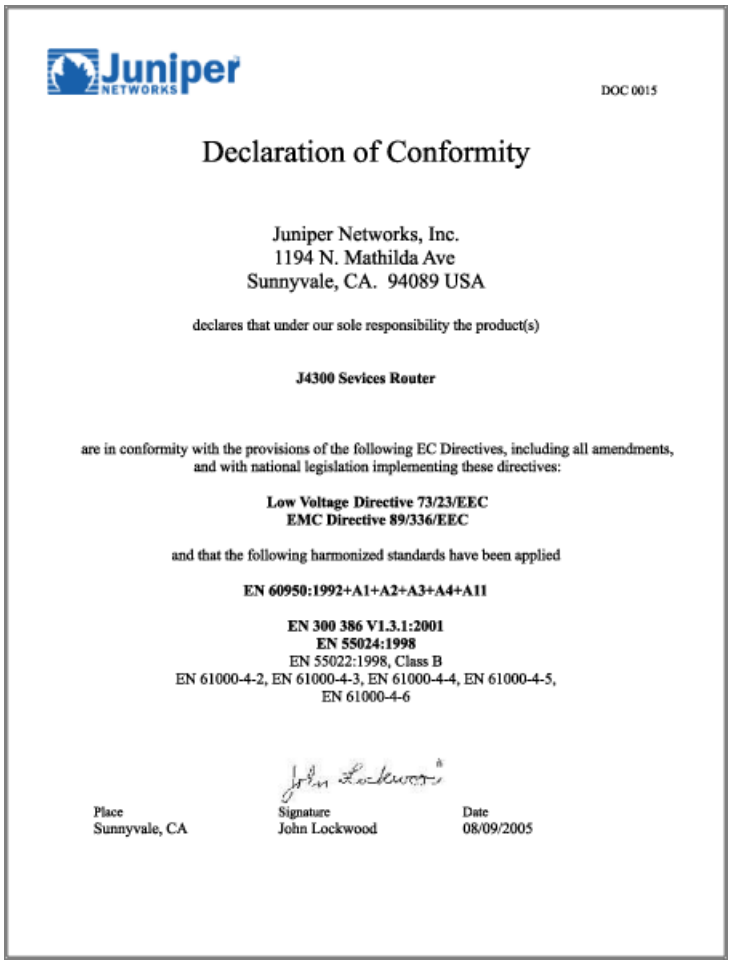
**Low Voltage Directive 73/23/EEC**
**EMC Directive 89/336/EEC**

and that the following harmonized standards have been applied

**EN 60950:1992+A1+A2+A3+A4+A11**

**EN 300 386 V1.3.1:2001**
**EN 55024:1998**
EN 55022:1998, Class B
EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6

| Place | Signature | Date |
|---|---|---|
| Sunnyvale, CA | John Lockwood | 08/09/2005 |



DOC 0015

# Declaration of Conformity

Juniper Networks, Inc.
1194 N. Mathilda Ave
Sunnyvale, CA. 94089 USA

declares that under our sole responsibility the product(s)

**J4300 Sevices Router**

are in conformity with the provisions of the following EC Directives, including all amendments, and with national legislation implementing these directives:

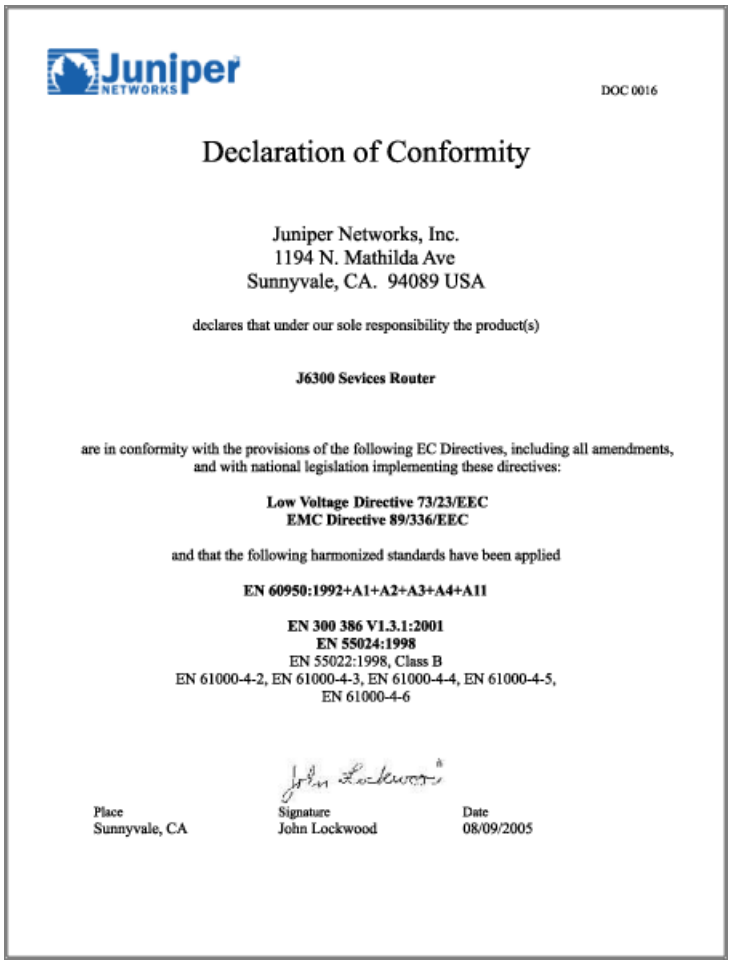
**Low Voltage Directive 73/23/EEC**
**EMC Directive 89/336/EEC**

and that the following harmonized standards have been applied

**EN 60950:1992+A1+A2+A3+A4+A11**

**EN 300 386 V1.3.1:2001**
**EN 55024:1998**
EN 55022:1998, Class B
EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6

| Place | Signature | Date |
|---|---|---|
| Sunnyvale, CA | John Lockwood | 08/09/2005 |



Juniper NETWORKS

DOC 0016

Declaration of Conformity

Juniper Networks, Inc.
1194 N. Mathilda Ave
Sunnyvale, CA. 94089 USA

declares that under our sole responsibility the product(s)

**J6300 Sevices Router**

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 60950:1992+A1+A2+A3+A4+A11**

**EN 300 386 V1.3.1:2001**
**EN 55024:1998**
EN 55022:1998, Class B
EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6

| Place | Signature | Date |
|---|---|---|
| Sunnyvale, CA | John Lockwood | 08/09/2005 |

### *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

# Part 5
# Index

# Index

## B



## C

## D

## E



## F

## G



## H

## I



## J

## K



## L

## M



## N



## O

## P

## Q



## R

## S

## T

## U



## V



## W

## X