C-series Platforms

C2000 and C4000 Hardware Guide

Release 3.1.x

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

Part Number: 530-028680-01, Revision 01

C-series Platforms Hardware Guide
Release 3.1.x

Writing: John Borelli
Editing: Fran Mues
Illustration: John Borelli
Cover Design: Edmonds Design

Revision History
13 February 2009—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 http://www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR 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 payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

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

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

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

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

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

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux 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)).

Table of Contents

About This Guide

SRC Guides and Release Notes

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with JUNOSe routers and JUNOS routing platforms in an Internet access environment. We assume that readers know how to use the routing platforms, directories, and RADIUS servers that they will deploy in their SRC networks.

If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

Table 1 on page xii defines the notice icons used in this guide. Table 2 on page xii defines text conventions used throughout this documentation.

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: Text Conventions

Convention	Description	Examples
Bold text like this	■ Represents keywords, scripts, and tools in text. ■ Represents a GUI element that the user selects, clicks, checks, or clears.	■ Specify the keyword **exp-msg**. ■ Run the **install.sh** script. ■ Use the **pkgadd** tool. ■ To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	user@host# **set cache-entry-age** *cache-entry-age*

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`}`

Regular sans serif typeface	■ Represents configuration statements. ■ Indicates SRC CLI commands and options in text. ■ Represents examples in procedures. ■ Represents URLs.	■ system ldap server{ stand-alone; ■ Use the request sae modify device failover command with the force option ■ user@host# . . . ■ http://www.juniper.net/techpubs/software/management/src/api-index.html
Italic sans serif typeface	Represents variables in SRC CLI commands.	user@host# **set local-address** *local-address*
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.

Table 2: Text Conventions *(continued)*

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	■ Emphasizes words. ■ Identifies book names. ■ Identifies distinguished names. ■ Identifies files, directories, and paths in text but not in command examples.	■ There are two levels of access: *user* and *privileged*. ■ *SRC-PE Getting Started Guide* ■ *o = Users, o = UMC* ■ The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Related Juniper Networks Documentation

With each SRC software release, we provide the *SRC Documentation CD*, which contains the documentation described in Table 3 on page xiii.

A complete list of abbreviations used in this document set, along with their spelled-out terms, is provided in the *SRC —PE Getting Started Guide*.

Table 3: Juniper Networks C-series and SRC Technical Publications

Document	Description
Core Documentation Set	
C2000 and C4000 Hardware Guide	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
C2000 and C4000 Quick Start Guide	Describes how to get the C-series Controller up and running quickly. Intended for experienced installers who want to expedite the installation process.
SRC-PE Getting Started Guide	Describes the SRC software, how to set up an initial software configuration, how to integrate RADIUS servers, and how to upgrade the SRC software. It also explains how to manage a C-series Controller. The guide describes how to set up and start the SRC CLI and the C-Web interface, as well as other SRC configuration tools. It includes reference material for the SRC documentation.
SRC-PE CLI User Guide	Describes how to use the SRC CLI, configure and monitor the platform with the CLI, and control the CLI environment. The guide also describes how to manage SRC components with the CLI.

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP	Describes how to use and configure the SAE, the NIC, and the SRC-ACP (Admission Control Plug-In) application. This guide also provides detailed information about using JUNOSe routers, JUNOS routing platforms, and other network devices in the SRC network.
SRC-PE Services and Policies Guide	Describes how to work with services and policies. The guide provides an overview, configuration procedures, and management information. The guide also provides information about the SRC tools for configuring policies.
SRC-PE Subscribers and Subscriptions Guide	Describes how to work with residential and enterprise subscribers and subscriptions. The guide provides an overview, configuration procedures, and management information. This guide also provides information about the enterprise service portals, including the Enterprise Manager Portal.
SRC-PE Monitoring and Troubleshooting Guide	Describes how to use logging, the SNMP agent, the SRC CLI, and the C-Web interface to monitor and troubleshoot SRC components. This guide also describes the SNMP traps.
SRC-PE Solutions Guide	Provides high-level instructions for SRC implementations. The guide documents the following scenarios: managing QoS services on JUNOSe routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); and mirroring subscriber traffic on JUNOSe routers.
SRC-PE CLI Command Reference, Volume 1 *SRC-PE CLI Command Reference, Volume 2*	Together constitute information about command and statement syntax; descriptions of commands, configuration statements, and options; editing level of statement options; and a history of when a command was added to the documentation.
SRC-PE NETCONF API Guide	Describes how to use the NETCONF application programming interface (API) to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software.
SRC-PE XML API Configuration Reference	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to configuration statements in the SRC command-line interface (SRC CLI).
SRC-PE XML API Operational Reference	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to operational commands in the SRC command-line interface (SRC CLI).
Application Library	
SRC Application Library Guide	Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, an application to provide threat mitigation, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, and an application to control volume usage .
Release Notes	

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
SRC-PE Release Notes *SRC Application Library Release Notes*	In the *Release Notes*, you will find the latest information about features, changes, known problems, resolved problems, supported platforms and network devices (such as Juniper Networks routers and CMTS devices), and third-party software. If the information in the *Release Notes* differs from the information found in the documentation set, follow the *Release Notes*. Release notes are available on the Web.

Obtaining Documentation

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

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the CD-ROM and DVD-ROM Documentation page at

http://www.juniper.net/techpubs/resources/cdrom.html

Copies of the Management Information Bases (MIBs) are available at http://www.juniper.net/.

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1
Product Overview

Chapter 1

C-series Controller Overview

This chapter provides introductory information about the C-series Controller. Topics include:

System Description

The C-series Controller enables you to easily install, configure, and support Juniper Networks Session and Resource Control-Policy Engine (SRC-PE) software. It provides easy access to troubleshooting information, such as reporting events, logs, and system dumps while providing session resource controller functionality.

There are two C-series Controller models: the C2000 model and the C4000 model. Each model is composed of two hard drives, fans, redundant power supplies, two USB ports, a console management port, and four Ethernet ports. The main difference between the two models is the number of service session licenses and concurrent subscribers allowed on each unit.

C-series Controller Models

Two C-series Controller models are available:

- C2000
- C4000

Both models use the same software. However, the specific model determines the number of service session licenses and concurrent subscribers allowed on each unit. (See Table 4 on page 3.)

Table 4: C-series Model Differences

Model	Concurrent Subscribers
C2000	200,000

Table 4: C-series Model Differences *(continued)*

Model	Concurrent Subscribers
C4000	500,000

NOTE: The models illustrated in this book might look different from your model because of configuration variations.

Figure 1: C2000, Front View

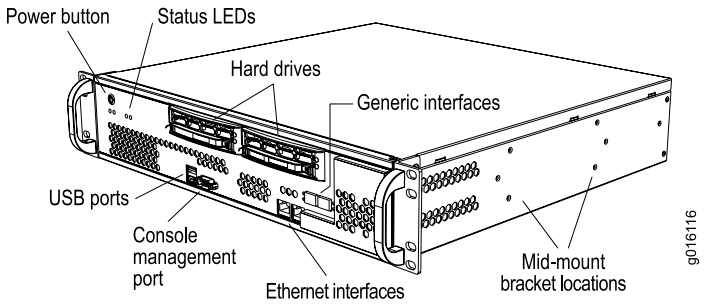


Figure 2: C2000, Rear View

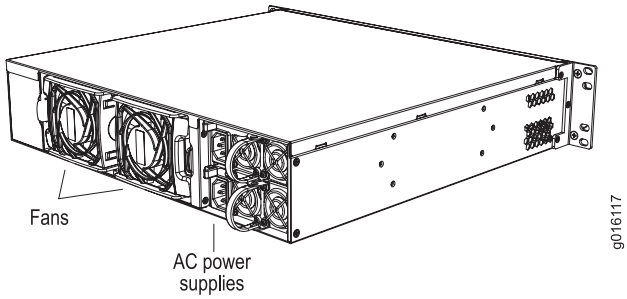


Figure 3: C4000, Front View

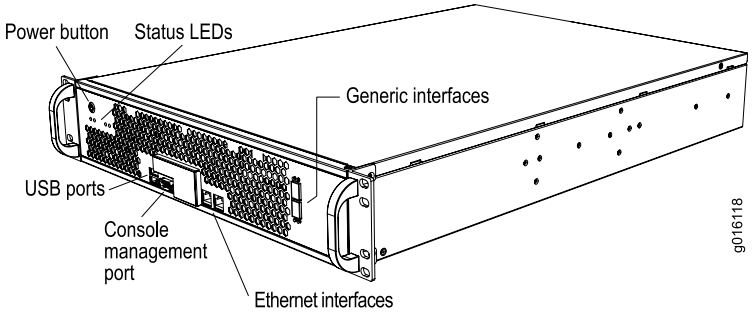
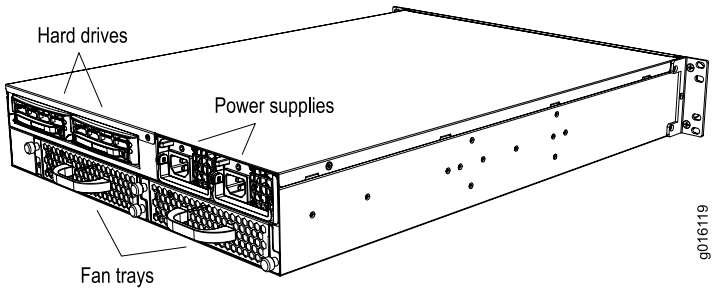


Figure 4: C4000, Rear View



C-series Model Components

The C2000 model and C4000 model contain the following components:

- Internal memory
- CPU
- Hard drive—Each model has two hot-swappable, redundant drives in a redundant array of independent disks (RAID) 1 (mirror) configuration. The C2000 model has two hard drives located in the front, and the C4000 model has two hard drives located in the rear.
- Fans—The C2000 model has two hot-swappable fans located in the rear. The C4000 model has two hot-swappable fan trays located in the rear. Each fan tray contains three fans.
- Power supply—Each model has two hot-swappable, redundant AC-power supplies located in the rear. Depending on the model, each power supply module has either two (C2000 model) or one (C4000 model) associated fan.

Figure 5: C2000 Power Supply

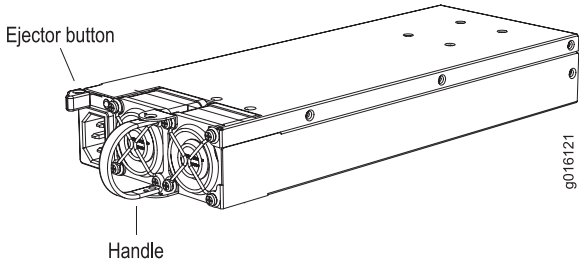
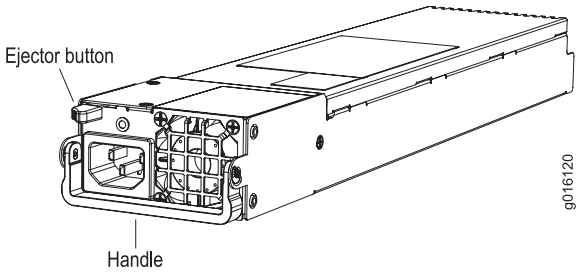


Figure 6: C4000 Power Supply



- Console management port—Each model has one RS-232 port that accepts a DB-9 (female) connector for direct CLI access from a console terminal.
- USB port—Each model has two ports that can be used for memory storage devices.
- Ethernet interfaces—Each model has two 10/100/1000Base-T Ethernet ports (ETH0 and ETH1) that accept an RJ-45 (male) connector, providing an out-of-band connection for LAN access through a Telnet session, SSH, or SNMP. ETH0 provides access from a network that is behind a firewall. ETH1 provides access for applications on an external network, such as the Internet.
- Generic interfaces—Each model has two generic ports (ETH2 and ETH3) that enable you to use standard connectors, such as small form-factor pluggable transceivers (SFPs), to create fiber-optic or Gigabit Ethernet connections and provide additional LAN connectivity. The following SFPs are available:
  - 1000Base-SX—Duplex LC connector, multimode, rated for 500 m over 10–micron core cable, 850-nm laser transmitter
  - 1000Base-LX—Duplex LC connector, single-mode, rated for 10 m over 10–micron core cable, 1310-nm laser transmitter
  - 1000Base-T—RJ-45 connector, rated for up to 100 m on CAT5 cable
- Status LEDs—Each model has LEDs that provide information about hard drive, power supply, and interface status.
- USB storage device—Contains the latest system software, including the operating system for the C-series Controller. The device is read-only and should be used to recover from a major software failure. See the *SRC Release Notes* for more information about recovering from a software failure.
- Rack-mount and rail kit.

Network Management Tools

You can use different management tools to configure the system to meet the specific networking requirements.

CLI Management

The command-line interface (CLI) provides fully developed and automated configuration and status functionality through a local RS-232 port, Telnet, or SSH

over any reachable network. For a full discussion of the CLI, see the *SRC–PE CLI User Guide*.

SNMP MIB Management

The system offers a complete SNMP interface for configuration, status, and alarm reporting. For more information, see *SRC–PE Monitoring and Troubleshooting Guide*.

Part 2
Initial Installation

Chapter 2

Unpacking and Inspecting the C-series Controller

This chapter reviews shipping contents and unpacking procedures for the C-series Controller. Topics include:

Before You Begin

Before you begin unpacking the item, be sure you have the following tools:

- A No. 2 Phillips screwdriver
- A utility knife
- A mechanical lift, or at least one person to assist in lifting

Unpacking the Units

The systems are delivered boxed. For your convenience, we recommend that you unpack the system in the location where you want to install it.

WARNING: Three people are required to install the system in a rack: two to lift it into position and one to screw it to the rack.

Inspecting System Components and Accessories

After you remove the equipment from the shipping containers:

- Confirm the contents of each container.
- Inspect all external surfaces and external connectors for visible signs of damage.

- Inspect all accessories shipped with each unit.
- Document any damage noted during your inspection.
- Confirm that the system has the correct number and type of components for your ordered configuration.

If You Detect or Suspect Damage

If you detect or suspect damage to any equipment:

- Contact the shipper responsible for delivery, and formally report the damage.
- Contact your Juniper Networks sales representative or reseller.

Contacting Juniper Networks

Please contact Juniper Networks at 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere), or contact your sales representative if you have any questions or concerns. See “Contacting Customer Support and Returning Hardware” on page 67 for complete contact information.

The Next Step

- To familiarize yourself with the electrical, environmental, and other guidelines and requirements for installing the system, see “Installation Guidelines and Requirements” on page 55.
- If you are familiar with these guidelines and requirements, see “Installing and Cabling the C-series Controller” on page 13.

Chapter 3

Installing and Cabling the C-series Controller

This chapter describes how to install the C-series Controller and attach cables. Topics include:

Before You Begin

Before installing the system, be sure you:

- Have a plan for installing the system that takes into consideration future expansion.
- Have the tools and accessories needed to complete the installation.
- Read and understand the clearance requirements for the front and back of the chassis for cable routing and other unit access. See "Environmental Requirements" on page 55 for more information.
- Read and understand the clearance requirements for the top and bottom of the chassis to ensure adequate ventilation.
- Prepare the equipment racks by measuring and marking space for each system you plan to install.

Freestanding Installation

When installing the system on a table top or in any other freestanding mode, be sure to leave enough space around the system for adequate ventilation. Position the system with easy access to the connections that it needs for power, local communications, and remote communications.

WARNING: Two people are required to lift the system.

CAUTION: To prevent electrostatic damage to the system and its components, make sure persons handling the system wear an antistatic device.

Rack-Mounted Installation

We recommend that you use a standard EIA distribution rack. See "Equipment Rack Requirements" on page 59 for rack information. You can install the system using the front or mid-mount brackets.

Installation Guidelines

Before installing the systems in a rack, consider the following guidelines:

- You can install several models in a single 7-ft. (2.1-m) rack. Installing multiple systems in a single rack enables you to maximize your available space.
- Install heavier systems on the bottom of the rack. Mount lighter systems higher in the rack.

Preparing the Equipment Racks

Following your installation plan, use a tape measure and marking pen to measure and mark space on each equipment rack for each system component. For horizontal spacing follow Network Equipment Building System (NEBS) requirements.

Installing the System

To complete the installation of the system in a rack, you need:

- A Phillips screwdriver
- Eight 10-32 x 3/8 Phillips screws (provided) for each model to be installed

To install the system in the rack:

1. If you are installing the system with the mid-mount brackets, use the provided screws to attach the brackets to the chassis. Use one bracket on each side. (See Figure 1 on page 4.)
2. With one person standing on the left side of the chassis and another standing on the right side, lift the unit into the rack.
3. Position the system in its designated location in the equipment rack. Make sure the holes of the mounting brackets align evenly with the holes of the equipment rack on both sides.

4. Starting at the bottom of the system, have the third person secure the system in the equipment rack by using the 10-32 x 3/8 Phillips screws.
5. Connect the necessary cables.

Cabling the System

Cabling the system requires the following main tasks:

1. Familiarize yourself with the ports, and ensure that you have the cables and wires needed to complete each cabling procedure.
2. Read and understand all safety warnings. (See “Installation Guidelines and Requirements” on page 55.)
3. Connect the system to the network and to a management console.
4. Connect the other interfaces to their appropriate network interface.
5. Connect the power cables from the power source to the system's power supply.

NOTE: We recommend that you use shielded cables where appropriate.

See “System Specifications” on page 35 for more information about system specifications.

Cabling the Management Console

Before powering up the system, you must set up a management console. The console enables you to communicate with your system during the power-up process and to manage your system using the command-line interface (CLI).

When connecting a console directly to the system, use a cable appropriate for your terminal connector. The cable must have a female DB-9 connector to attach to the RS-232 port on the system.

Management Ports

The management section of the system has three ports for management access (see Figure 7 on page 17 and Figure 9 on page 17):

- Two 10/100Base-T Ethernet ports—Each accepts an RJ-45 (male) connector, providing an out-of-band connection for LAN access through a Telnet session, SSH, or SNMP.
- One RS-232 management port—Accepts a DB-9 (female) connector. This port provides direct CLI access from a console terminal.

The management port is considered a data terminal equipment (DTE) interface. Direct connection to a terminal or PC (which also has DTE interfaces) requires a crossover cable.

See “Setting the Initial Configuration” on page 21 for more information about management access.

Connecting to the Network

To connect the system to the network:

1. Insert an Ethernet cable (RJ-45) connector into the 10/100Base-T (RJ-45) port on the system until it clicks into place.
2. Connect the other end of the cable to the appropriate Ethernet network for an out-of-band connection.

Connecting to a Console Terminal

When you connect a console directly to the system, use a cable appropriate for your terminal connector. The cable must have a female DB-9 connector to attach to the RS-232 port on the system.

To connect the console:

1. Insert the female DB-9 connector into the RS-232 port, and tighten the screws.
2. Connect the other end of the cable to your terminal's serial port (VT100/ANSI).

Cabling Ethernet Interfaces

Port ETH0 and ETH1 on the C2000 model and the C4000 model accept RJ-45 10/100/1000Base-T Ethernet (copper) interfaces. Port ETH2 and port ETH3 on the C2000 model and the C4000 model accept SFPs.

Cabling the System for Power

After you have correctly cabled the system, you can then attach the power cord. See Figure 8 on page 17 and Figure 10 on page 17. See “System Specifications” on page 35 for the power requirements for the system.

To cable the system for power:

1. Insert the power cord into the AC power IEC receptacle.
2. Insert the other end of the power cord into an appropriate AC power source.

NOTE: We suggest that you use an uninterruptible power supply (UPS) with your C-series Controller.

NOTE: To provide redundancy, do not terminate Power A and Power B leads at the same power source.

Figure 7: C2000, Front View

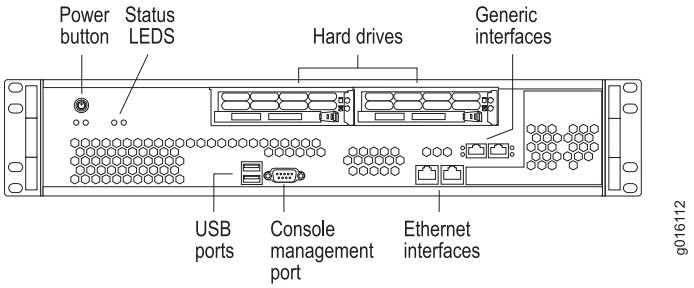


Figure 8: C2000, Rear View

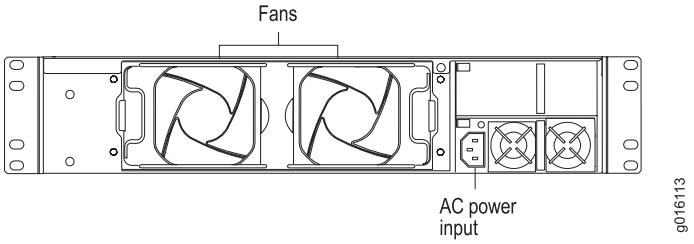


Figure 9: C4000, Front View

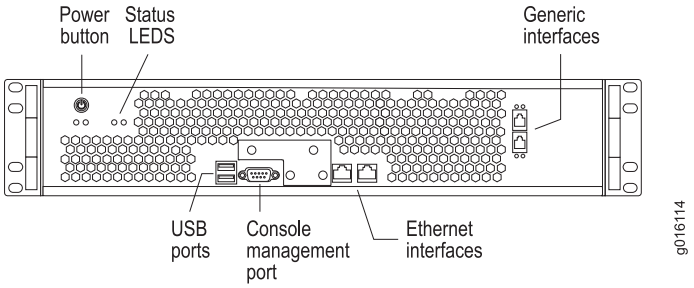
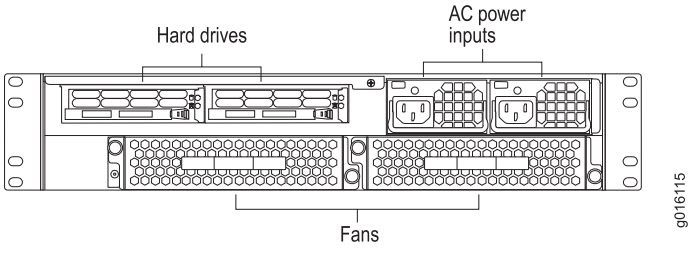


Figure 10: C4000, Rear View



The Next Step

After you finish installing and cabling the system:

- See “Powering Up the C-series Controller” on page 19.

Chapter 4

Powering Up the C-series Controller

This chapter describes how to power up the C-series Controller. Topics include:

Powering Up

NOTE: In this procedure we assume that the system is already connected to a power source.

For specifications of the electrical requirements for the system, see "System Specifications" on page 35.

CAUTION: Evaluate the overall loading of the branch circuit before you install any equipment into a rack.

To power up the system:

1. Verify that the power source is operational and turned on.
2. Inspect all grounding and power connections to the system.
3. Confirm that all connections are secure.
4. Push the PWR button.
5. Monitor the LEDs to verify that the system is booting properly.

   When the prompt appears on the system console, you can log in and configure the system.

See the "Setting the Initial Configuration" on page 21 and *SRC-PE CLI User Guide* for more information.

Status LEDs

The LEDs listed in Table 5 on page 20 are used on both models.

Table 5: Model LEDs

LED Label	LED Indicator	LED Color	OFF to ON	ON to OFF
PWR	Power	Green	Power on	Power off
HD	Hard drive		Hard drive is functioning	Hard drive failure detected
TEMP	Temperature	Red	Temperature error exists; fan failure	Fan okay
PS FAIL	Power supply failure	Red	Failure detected	Fan okay
LINK	Ethernet	Green	Ethernet link up	Ethernet link down
TX/RX	Ethernet	Green	Blinks when Ethernet traffic on link	No Ethernet traffic on link

The Next Step

See “Setting the Initial Configuration” on page 21.

Chapter 5

Setting the Initial Configuration

This chapter discusses how to set up the C-series Controller after powering it on. For basic information on the management of the system, see the *SRC-PE Getting Started Guide*. Topics include:

Configuration Overview

After powering on the system, there are six main steps required to get it ready to work with:

1. Connect a management console to the system, configure it, and log in.
2. Configure the Juniper Networks Database.
3. Configure hostname and domain information.
4. Configure the system for remote access.
5. Configure the system to accept SSH and Telnet connections.
6. Add an Admin user account.

Setting Up Management Access and Logging In

Before you power up the system, you must set up a management console. (See "Connecting to a Console Terminal" on page 16.)

You can monitor and manage the system through either of these methods:

- Console terminal—Connect a console (PC, Macintosh, or UNIX workstation) directly to the system's RS-232 serial port.

- Remote console—Connect 10/100Base-T port (ETH0) to an Ethernet network, and run SSH or Telnet from a remote console.

For initial access to the system, you need to physically connect your console directly to the system's RS-232 port. Through this connection you use the SRC command-line interface (CLI) to set the hostname and domain information. You can then access the system remotely (for example, by means of SSH).

To communicate with the system, you must have a terminal emulation program running on your PC or Macintosh. You can use any terminal emulation program, such as HyperTerminal. A UNIX workstation can use the emulator TIP.

To log in to the system:

1. Start your terminal emulation program using the following settings:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: none
2. Enter the username.

   ```
   SRC-PE Release 7.0 [B.7.0.0-12]
   localhost login:root
   ```

3. Enter the password.

   ```
   localhost password:password
   — SRC CLI 7.0 build CLI.B.7.0.0.012
   (c) 2005-2007 Juniper Networks Inc.
   root@localhost>
   ```

   You are now logged in as root user.

Configuring the Juniper Networks Database

Each C-series Controller contains a Juniper Networks database. The database stores SRC data, sample data, configuration information, and user profiles. You must enable the Juniper Networks database the first time you power on the system. It can operate as a standalone database or as a member of a community of Juniper Networks databases.

NOTE: The Juniper Networks database must be running before you start configuring the SRC software.

Typically, you run the database in standalone mode only in testing environments. In standalone mode, the database does not communicate with other Juniper Networks

databases; there is no data distribution and no redundancy. In community mode, databases distribute data changes among specified databases. When you have two or more C-series Controllers, enable the Juniper Networks database to run in community mode, and assign a role to each database:

- Primary role—A database that provides read and write access to client applications. It replicates its data and distributes changes to any Juniper Networks databases configured as neighbors.
- Secondary role—A database that provides read access to client applications. If client applications try to write data to this database, the database refers the client to a primary database.

In the following example, a standalone database is enabled. For more information about community mode, see *SRC-PE Getting Starting Guide, Chapter 10, Managing the Juniper Networks Database*.

To enable a Juniper Networks database to run in standalone mode:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database.

   ```
   user@host# edit system ldap server
   ```

2. Enable standalone mode.

   ```
   [edit system ldap server]
   user@host# set stand-alone
   ```

Configuring Hostname and Domain Parameters

To set hostname and domain parameters:

1. Enter configuration mode.

   ```
   root@host> edit
   ```

2. Configure the hostname.

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

   For example:

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

3. Configure either a list of domain names to search, or create the domain name. We recommend configuring a list of domain names to search.

   To configure a list of domain names to search:

   ```
   [edit]
   root@host# set system domain-search [domain-name1, domain-name2, ...]
   ```

For example:

```
[edit]
root@host# set system domain-search [my-domain.juniper.net
   domain.juniper2.net]
```

To configure the domain name:

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

For example:

```
[edit]
root@host# set system domain-name my-domain.juniper.net
```

Configuring the System for Remote Access

To allow remote access to the system, you must configure the generic interfaces. You can specify an IP address with mask or a broadcast address with mask for an interface. For more information, see *SRC–PE Getting Starting Guide, Chapter 7, Configuring Remote Access to an SRC Platform*.

To configure the generic interfaces:

1. From configuration mode, access the configuration statement that configures the interface.

   ```
   user@host# edit interfaces eth0
   ```

2. Specify the unit, family, and IP address for the interface.

   ```
   [edit interfaces eth0]
   user@host# set unit number family inet address address
   ```

   For example, to configure an interface with only an IP address:

   ```
   [edit interfaces eth0]
   user@host# set unit 0 family inet address 192.2.0.10/24
   ```

3. (Optional) Specify the broadcast address for the interface.

   ```
   [edit interfaces eth0]
   user@host# set unit number family inet broadcast broadcast
   ```

   For example, to configure an interface with only a broadcast address:

   ```
   [edit interfaces eth0]
   user@host# set unit 0 family inet broadcast 192.2.0.255
   ```

4. Verify the interface configuration.

   ```
   [edit interfaces eth0]
   user@host# show
   unit 0 {
   ```

```
family {
   inet {
      broadcast 192.2.0.255;
   }
}
}
```

Configuring the System to Accept SSH and Telnet Connections

You can enable SSH and Telnet to let users who have the appropriate privileges connect to the system. For security reasons, we recommend that you do not allow remote users to access the CLI as root. The system does not allow root access over a Telnet connection. For more information, see *SRC-PE Getting Starting Guide, Chapter 7, Configuring Remote Access to a C-series Controller with the SRC CLI*.

To configure the system to accept SSH connections:

1. From configuration mode, access the [edit system services ssh] hierarchy level.
2. (Optional) Specify whether or not to allow root login through SSH.

   ```
   [edit system services ssh]
   user@host> set root-login (allow | deny | deny-password)
   ```

   where:

   - allow— Allow users to log in to the C-series Controller as root through SSH.
   - deny— Disable users from logging in to the system as root through SSH.
   - deny-password— Allow users to log in to the system as root through SSH when the authentication method (for example, RSA authentication) does not require a password. (Default)

To configure the system to accept Telnet connections:

- In edit mode, type the following command.

  ```
  [edit]
  user@host# set system services telnet
  ```

Adding an Admin User Account

Although root access is used for initial configuration of the system, user accounts are used to enter commands and statements at the CLI. Therefore, you must set up an admin account to allow further configuration. You can use a built-in class, such as super-user.

To configure an account for an administrative user:

1. Create an account for an administrative user.

   ```
   [edit]
   ```

```
user@host # edit system login user user
```

For example:

```
[edit]
user@host # edit system login user myadmin
```

2. Set the class for the administrative user to the login class that you created.

```
[edit system login user myadmin]
user@host # set class class
```

For example:

```
[edit system login user myadmin]
user@host # set class super-user
```

3. Specify the name of the administrative user.

```
[edit system login user myadmin]
user@host # set full-name “John Doe”
```

4. Set the CLI editing level to expert.

```
[edit system login user myadmin]
user@host# set level expert
```

5. (Optional) Specify that a space be used for command completion.

```
[edit system login user myadmin]
user@host # set complete-on-space on
```

6. Verify that the configuration for the administrative user is correct.

```
[edit system login user myadmin]
user@host# show
class super-user;
full-name "John Doe";
uid 506;
gid 100;
level expert;
complete-on-space on;
```

7. Set the password of the user.

```
[edit]
user@host# edit system login user myadmin authentication
[edit system login user myadmin authentication]
user@host# set plain-text-password
```

The Next Step

See “Maintaining the System” on page 29.

Part 3

Hardware Maintenance Procedures and Specifications

Chapter 6

Maintaining the System

This chapter lists the tools, items, and steps needed for installing and uninstalling components. Other maintenance procedures must be performed by an authorized Juniper Networks technician. Topics include:

Required Tools and Items

You need the following tools and other items to replace components:

- Flathead and Phillips screwdrivers
- Insulated adjustable wrench
- Antistatic wrist strap
- Antistatic bags (or other protective packaging to hold components)
- Plastic boots or other protective covers for fiber-optic connectors

Storing Modules and Components

Retain the packaging in which a component was shipped, and use this packaging to store the item.

CAUTION: Failure to store electronic components correctly can lead to damage of these items.

Follow these guidelines for storing components:

- Store each component in a separate antistatic bag.
- Store components in an antistatic plastic container. Some of these containers can accommodate several components in separate compartments.
- Do not store multiple components in an antistatic bag or container where they can touch other items.
- (Optional) Store the item in its antistatic bag or container within the protective packaging or padded box that the item was shipped in.

Cleaning the System

Clean the system with a dry cloth every few weeks to prevent excessive dust accumulation. This cleaning helps to maintain the efficiency of the cooling system and to prevent damage to electronic components.

WARNING: Do not insert any metal object, such as a screwdriver, or place your hand into an open slot when the system is on. Remove jewelry (including rings, necklaces, and watches) before working on equipment that is connected to power lines. These actions prevent electric shock and serious burns.

CAUTION: When cleaning the system, wear an antistatic device. This action helps to protect components from damage by electrostatic discharge.

Installing or Replacing an SFP

This section describes how to install or replace an SFP. SFPs can be installed in either generic interface port (ETH2 or ETH3). See Figure 11 on page 30 and Figure 12 on page 31 for generic interface port locations.

When replacing an SFP, make sure that you open the ejector handle completely before gently pulling it out of the interface.

Figure 11: C2000, Front View

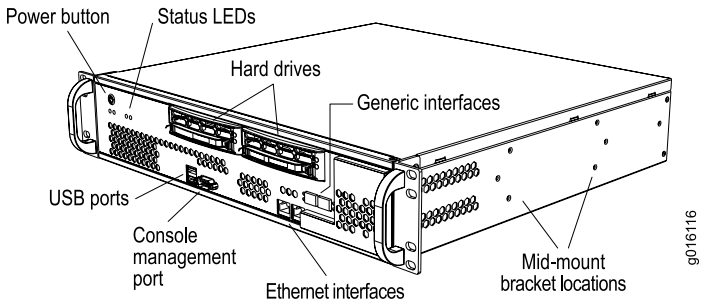
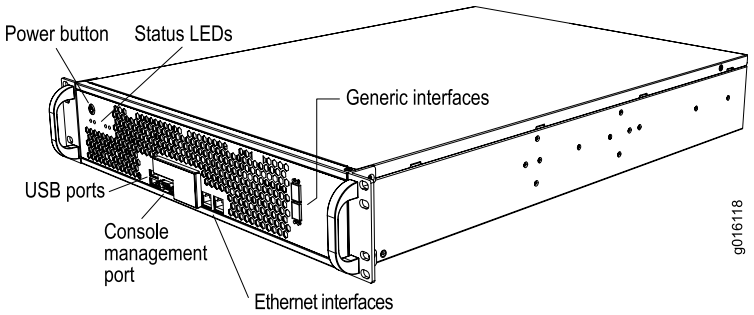


Figure 12: C4000, Front View



Tools and Parts Required

To remove and replace an SFP, you need the following tools and parts:

- Electrostatic bag or antistatic mat, one for each SFP removed
- ESD grounding wrist strap
- Rubber safety caps to cover each unused cable and SFP

Removing an SFP

To remove an SFP:

1. Have a replacement SFP or a transceiver slot plug ready, as well as an antistatic mat and a rubber safety cap for the SFP.
2. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to an appropriate grounding point.
3. Label the cables connected to the SFP so that you can reconnect them correctly later.

WARNING: Do not look directly into a fiber-optic transceiver or into the end of a fiber-optic cable. Fiber-optic transceivers contain laser light sources that can damage your eyes.

---

4. Remove the cable connector plugged into the SFP.

CAUTION: Avoid bending fiber-optic cable beyond its minimum bend radius. An arc smaller than a few inches in diameter can damage the cable and cause problems that are difficult to diagnose.

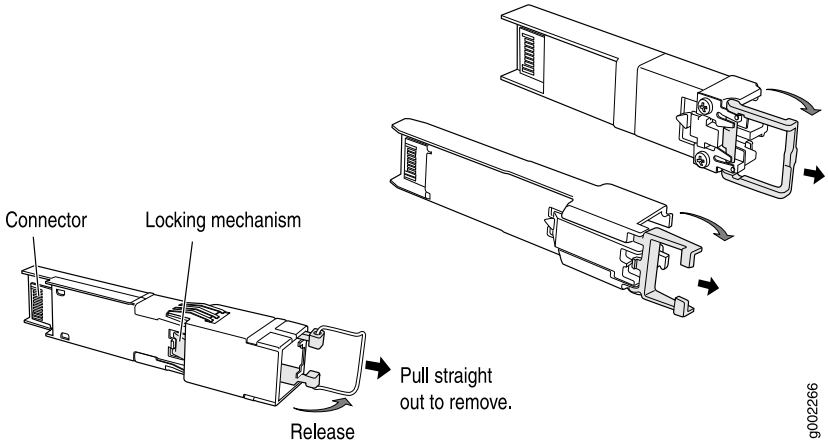
---

5. Pull the ejector handle out from the SFP to unlock the SFP.

CAUTION: Make sure that you open the ejector handle completely (you will hear it click). This prevents damage to the SFP.

6. Grasp the SFP ejector handle, and pull the SFP approximately 0.5 in (1.3 cm) out of the interface port.
7. Using your fingers, grasp the body of the SFP, and pull it the rest of the way out.

Figure 13: Removing SFPs



8. Place a rubber safety cap over the transceiver.
9. Place the removed SFP on an antistatic mat or in an electrostatic bag.

Installing an SFP

To install an SFP:

1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to an appropriate grounding point.
2. Take each SFP to be installed out of its electrostatic bag, and identify the interface where it will be installed.
3. Verify that each transceiver is covered by a rubber safety cap. If it is not, cover the transceiver with a safety cap.
4. Carefully align the SFP with the interface. The connectors should face the chassis.
5. Slide the SFP until the connector is seated in the interface. If you are unable to fully insert the SFP, make sure the connector is facing the right way.
6. Remove the rubber safety cap from the transceiver and the end of the cable. Insert the cable into the transceiver.

Removing and Installing a Fan

Both C-series models have two cooling fans that provide forced air cooling for components in the system. Each fan is hot-swappable; you can replace it without powering down the system. You can monitor fan status by observing the TEMP LED.

NOTE: If the red TEMP LED is illuminated, either a critical or noncritical failure exists.

CAUTION: If the TEMP LED is illuminated and none of the fans is spinning, quickly power down the system until a new set of fans is available. Operating a system with inadequate air circulation can damage the components.

To remove a fan:

1. Unlock or loosen the fan from the system.
   - For the C2000 model, press the locking tab and rotate the fan away from the system.
   - For the C4000 model, loosen the thumb screw in the top-left and lower-right of the fan.
2. Pull the fan out and remove it from the system.

   Use two hands to hold the fan after it comes out of the chassis.

WARNING: Do not place your fingers near the fans when removing the unit. The blades might still be moving.

CAUTION: Do not use the fan tray handle to carry the fan. Use the handle only to push the tray into the chassis or pull it out.

To install a fan, reverse the steps taken to remove the fan.

Removing and Installing a Power Supply Module

NOTE: If your system is powered on, see the *SRC–PE CLI User Guide, Chapter 5, Using the SRC CLI Operational Commands to Monitor the SRC Software* for commands to run before performing these steps.

To remove a power supply module:

1. Unplug the power cord.

2. Slide the locking tab (ejector button) to the left to release the module. See Figure 14 on page 34 and Figure 15 on page 34.
3. Hold the tab to the left, and using the handle, slowly pull the power supply module out.

To install a power supply module:

1. Hold the locking tab (ejector button) to the left, and slowly slide the module into the chassis until it clicks into place.
2. Insert the power cord into the AC power IEC receptacle.

Figure 14: C2000 Power Supply

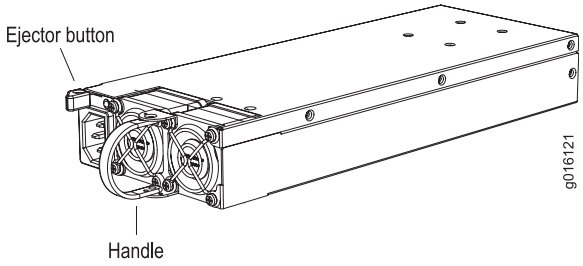
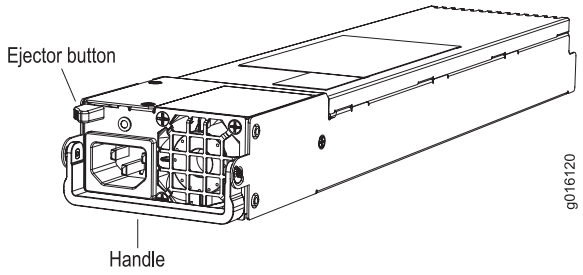


Figure 15: C4000 Power Supply



Removing and Installing a Hard Drive

NOTE: If your system is powered on, see the *SRC-PE Getting Started User Guide* for commands to run before performing these steps.

To remove a hard drive:

1. Slide the locking tab in the bottom-right corner to the right to release the hard drive.
2. Hold the tab to the right and slowly pull the unit out.

To install a hard drive, hold the locking tab to the right and slowly slide the unit into the chassis until it clicks into place.

Chapter 7

System Specifications

This chapter lists the system specifications, requirements, and certifications for the system. Topics include:

C2000 Model Specifications

Table 6: C2000 Model Specifications

Category	Specification
Weight	33 lb (15 kg)
Dimensions	3.5 (H) x 16.7 (W) x 16.2 (D) inches 8.89 (H) x 42.42 (W) x 41.15 (D) cm
Environmental Requirements	
Temperature	■ Operating: 50° to 104° F (10° to 40° C) ■ Storage: –40° to 158° F (–40° ˚ to 70° C)
Relative humidity	■ Operating: 8% to 90% (noncondensing) ■ Storage: 5% to 95% (noncondensing)
Heat Dissipation	500 W, 1706 BTU/hour maximum
AC Input	
Power required	■ 90-132 VAC (115V Nominal), 47–63 Hz ■ 180–264 VAC (230V Nominal), 47–63 Hz
Power	500 W
Efficiency	65% minimum at full load
DC Input	
Voltage	-36V to -75 VDC
Current	-48 V nominal
Power	500 W

Table 6: C2000 Model Specifications *(continued)*

Category	Specification
Efficiency	70% minimum at full load
Space Requirements	■ 3 feet (90 cm) behind system or rack. ■ Do not block air vents on front or back of the system.
Safety Agency Certification	■ CAN/CSA-C22.2 No. 60950-1-03 ■ EN 60950-1:2001 + A11 ■ EN 60825-1:1994 + A1 + A2 ■ Low Voltage Directive 73/23/EEC ■ UL 60950-1:2003
Airflow	■ Air intake occurs in the front of the system. ■ Air is exhausted out of the rear of the system.
Electromagnetic Emissions Agency Certification	■ AZ/NZS CISPR 22:2002 ■ EMC Directive (89/336/EEC) ■ EN 300 386 V1.3.3:2005 ■ EN 300 386 V1.3.3:2005 ■ EN 55022:1998 + A1 (2000) + A2(2003) Class A ■ EN 55024: 1998 + A1: 2001 + A2: 2003 ■ EN 61000-3-2:2001 ■ EN 61000-3-3:1995 ■ FCC Part 15 Subpart B ■ VCCI (Voluntary Control Council for Interference by Information Technology Equipment)

C4000 Model Specifications

Table 7: C4000 Model Specifications

Category	Specification
Weight	48 lb (22 kg)
Dimensions	3.5 (H) x 16.7 (W) x 24 (D) inches 8.89 (H) x 42.42 (W) x 60.96 (D) cm
Environmental Requirements	
Temperature	■ Operating: 50° to 104° F (10° to 40° C) ■ Storage: –40° to 158° F (–40° ˚ to 70° C)
Relative humidity	■ Operating: 8% to 90% (noncondensing) ■ Storage: 5% to 95% (noncondensing)
Ambient storage temperature	–40° ˚ to 158° F (–40° ˚ to 70° C), 95% relative humidity

Table 7: C4000 Model Specifications *(continued)*

Category	Specification
Ambient storage humidity	5% to 95% (noncondensing)
Heat Dissipation	700 W, 2389 BTU/hour maximum
AC Input	
Power required	90-264 VAC, 47–63 Hz
Power	700 W
Efficiency	80% minimum at full load
Space Requirements	■ 3 feet (90 cm) behind system or rack. ■ Do not block air vents on or back of the system.
Airflow	■ Air intake occurs in the front of the system. ■ Air is exhausted out of the rear of the system.
Safety Agency Certification	■ CAN/CSA-C22.2 No. 60950-1-03 ■ EN 60950-1:2001 + A11 ■ EN 60825-1:1994 + A1 + A2 ■ Low Voltage Directive 73/23/EEC ■ UL 60950-1:2003
Electromagnetic Emissions Agency Certification	■ AZ/NZS CISPR 22:2002 ■ EMC Directive (89/336/EEC) ■ EN 55022:1998 + A1 (2000) + A2(2003) Class A ■ EN 55024: 1998 + A1: 2001 + A2: 2003 ■ EN 61000-3-2:2001 ■ EN 61000-3-3:1995 ■ FCC Part 15 Subpart B ■ VCCI (Voluntary Control Council for Interference by Information Technology Equipment)

Chapter 8

Managing RAID Disks on a C-series Controller

This chapter describes how to manage and view status information for RAID disks on a C-series Controller. Topics include:

C-series Controller Data Storage

A C-series Controller provides data redundancy by supplying two hard drives (or disks) in a redundant array of independent disks (RAID). Both disks are configured as a RAID-1 mirror; this means that data is concurrently written to both disks. If one disk becomes inoperable, the remaining disk continues to be active, which allows the C-series Controller to continue to function.

When you replace a faulty disk and initialize it, or disable and then enable a disk, the RAID controller copies all the data from the active disk to the enabled or initialized disk and establishes mirroring for the two disks.

The location of the disk mount for the disks depends on the model of the C-series Controller:

- C2000 system—Front of chassis
- C4000 system—Back of chassis

When you access the disks in the disk mount:

- Disk 0 is to the left.
- Disk 1 is to the right.

You can also use the **request disk identify** command to make the LED for a specified disk blink to verify which disk is disk 0 and which is disk 1.

Managing Disks in a C-series Controller

The SRC CLI provides commands to let you monitor disk status, replace faulty disks, and reinitialize disks in the system.

Replacing or Swapping a Disk

You can replace a failed disk or swap a working disk in a C-series Controller. Note the following limitations:

- Replacing a disk— You can replace it while the other disk remains active.
- Swapping a disk—You cannot remove both disks in the C-series Controller at the same time. Do not power down the system or initialization errors may occur.

To replace or swap a disk:

1. Disable the disk.

   user@host> **request disk disable device** 0 | 1

NOTE: Do not power down the C-series Controller when you are swapping a disk, because doing so might result in initialization errors.

2. Remove the disk from the system.
3. Insert a new disk.
4. Enable the disk.

   user@host> **request disk enable device** 0 | 1

5. Initialize the new disk.

   user@host> **request disk initialize device** 0 | 1

   The command generates data on the disk that enables the disk controller to manage the disk. The disk controller copies data from the other disk and establishes mirroring between the two disks.

6. Verify that the disk is initialized.

   user@host> show disk status

```
C:ID:L  Device Type     Blocks    Bytes/Block Usage            Shared Rate
------  --------------  --------- ----------- ---------------- ------ ----
0:00:0   Disk            145226112 512         Initialized      NO     150
0:01:0   Disk            145226112 512         Initialized      NO     150

        Smart    Method of         Enable
        Capable  Informational     Exception  Performance  Error
C:ID:L  Device   Exceptions(MRIE)  Control    Enabled      Count
------  -------  ----------------  ---------  -----------  ------
```

```
0:00:0     Y            6             Y           N             0

0:01:0     Y            6             Y           N             0

Controller Tasks

TaskId Function  Done%  Container State Specific1 Specific2

------ -------- ------- --------- ----- --------- ---------
100     Rebuild  0.3%    0         RUN   00000000  00000000
```

Reinitializing an Active Disk

You can reinitialize a disk that is already active in a C-series Controller.

To reinitialize a disk:

- Initialize the disk.

  user@host> **request disk initialize device** 0 | 1 **force**

  The command generates data on the disk that enables the disk controller to manage the disk. The disk controller copies data from the other disk and establishes mirroring between the two disks.

Viewing Information About Disks on a C-series Platform

To view information about disks in the C-series Controller:

- Enter the show disk status command.

  user@host> **show disk status**

```
C:ID:L  Device Type     Blocks    Bytes/Block Usage            Shared Rate

------  --------------  --------- ----------- ---------------- ------ ----

0:00:0   Disk            145226112 512         Initialized      NO     150

0:01:0   Disk            145226112 512         Initialized      NO     150

        Smart    Method of         Enable

        Capable  Informational     Exception  Performance  Error

C:ID:L  Device   Exceptions(MRIE)  Control    Enabled      Count

------  -------  ----------------  ---------  -----------  ------

0:00:0     Y            6             Y           N             0

0:01:0     Y            6             Y           N             0
```

```
Controller Tasks

TaskId Function  Done%  Container State Specific1 Specific2

------ -------- ------- --------- ----- --------- ---------
No tasks currently running on the controller
```

Table 8: show disk status Output Fields

Field Name	Field Description
C:ID:L	C indicates the channel number, ID the device ID, and L the device logical number
Device Type	Type of device; disk
Blocks	Number of blocks available on the disk
Bytes/Block	Number of bytes for each block
Usage	Status of disk: ■ Detached—Not available for use ■ Initialized—Prepared for use with arrays ■ Not initialized—Not prepared for use with arrays ■ Offline—Present at system boot, but the disk was removed or failed ■ Unowned—The controller does not control the disk
Shared	Whether or not the disk is on a shared channel
Rate	Disk speed in megabytes per second
Smart Capable Device	Whether or not the device is enabled for Specifies if Self-Monitoring, Analysis and Reporting Technology (SMART)
Methods of Informational Exceptions (MIE)	List of MIE exceptions
Enable Exception Control	Whether or not SMART exception reporting is enabled
Performance Enabled	Whether or not performance is enabled
Error Count	Number of errors that SMART found on the disk
Controller Tasks	The **No tasks currently running on controller** message indicates that no tasks are running, including initialization.

Chapter 9

Configuring IPMI on a C-series Platform (SRC CLI)

This chapter describes how to configure IPMI on a C-series platform with the SRC CLI. Topics include:

Overview of IPMI

Intelligent Platform Management Interface (IPMI) is a message-based hardware management interface that enables remote monitoring, management, and recovery capabilities, regardless of the status of the server. It defines a set of interfaces that are common to computer hardware and firmware that you can use to monitor system health and manage the system.

IPMI operates independently of the operating system (OS) and allows you to manage a system remotely even in the absence of the OS or the system management software, or even if the monitored system is not powered on. IPMI can also function when the OS has started.

IPMI version 1.5 and later can send out alerts by means of a direct serial connection, a LAN, or a serial over LAN (SOL) connection to a remote client. You can then query controller status, review hardware logs, or issue other requests from a remote console through the same connections.

Commands to Manage an IPMI Interface

You can use the following operational mode commands to manage IPMI interfaces:

- ipmisol open
- ipmisol close remote-session
- ipmisol close local-session

For detailed information about each command, see the *SRC-PE CLI Command Reference*.

Configuring IPMI with the SRC CLI

For the C2000 model, an IPMI configuration includes an IP address assigned to the IPMI interface and a gateway IP address. For the C4000 model, only a gateway IP address is required because the IP address for the IPMI interface is the same as the IP address assigned to the eth0 interface on the C4000 model.

Use the following configuration statements to configure an IPMI interface on a C-series Controller:

```
system ipmi {
    address address;
    gateway gateway;
    user name;
}
```

To configure IPMI on an interface:

1. From configuration mode, access the configuration statement that configures an IPMI interface.

   ```
   user@host# edit system ipmi
   ```

2. Set the IP address.

   ```
   [edit system ipmi]
   user@host# set address address/destination prefix
   ```

   An IP address is required for a C2000 model but is set automatically to the address of the eth0 interface on a C4000 model.

3. Set the default gateway IP address. A default gateway is a node on a network that serves as an access point to another network.

   ```
   [edit system ipmi]
   user@host# set gateway gateway
   ```

4. Verify the configuration.

   ```
   [edit system ipmi]
   user@host# show
   address 10.227.7.145/24;
   gateway 10.227.7.1;
   ```

Viewing IPMI Chassis Information

You can view IPMI chassis information for the controller you are currently logged in to and for a remote controller. You must be logged on as a root user.

To display the chassis information on the local controller using IPMI:

1. Log in as root user.

   ```
   SRC-PE Release 3.1 [R.3.1.0-12]
   login: root
   ```

2. Enter the password.

   ```
   Password: password
   — SRC CLI 3.1 build CLI.R.3.1.0.012
   (c) 2005-2008 Juniper Networks Inc.
   root@host>
   ```

   You are now logged in as root user.

3. Enter the show ipmi chassis command.

   For example:

   ```
   root@host>show ipmi chassis


   System Power         : on
   Power Overload       : false
   Power Interlock      : inactive
   Main Power Fault     : false
   Power Control Fault  : false
   Power Restore Policy : always-off
   Last Power Event     :
   Chassis Intrusion    : inactive
   Front-Panel Lockout  : inactive
   Drive Fault          : false
   Cooling/Fan Fault    : false


   System Power         : on
   Power Overload       : false
   Power Interlock      : inactive
   Main Power Fault     : false
   Power Control Fault  : false
   Power Restore Policy : always-off
   Last Power Event     :
   Chassis Intrusion    : inactive
   Front-Panel Lockout  : inactive
   Drive Fault          : false
   Cooling/Fan Fault    : false
   ```

To display the IPMI chassis information on a remote controller:

1. Log in as root user.
2. Enter the show ipmi host chassis command.

user@host>**show ipmi host** *host* **user** *user* **chassis**

- host—IP address of remote host IPMI interface
- user—IPMI username configured in the remote host

For example:

root@host>**show ipmi host 10.10.10.30 user johndoe chassis**

Viewing Power Status of a Controller Using IPMI

You can view IPMI power information for the controller you are currently logged on to and for a remote controller. You must be logged in as a root user.

To display power status (on or off) of the local controller using IPMI:

1. Log in as root user.

   SRC-PE Release 3.1 [R.3.1.0-12]
   login: **root**

2. Enter the password.

   Password: **password**
   — SRC CLI 3.1 build CLI.R.3.1.0.012
   (c) 2005-2008 Juniper Networks Inc.
   root@host>

   You are now logged in as root user.

3. Enter the show ipmi power command.

   For example:

   ```
   root@host>show ipmi power

   Chassis Power is on
   ```

To display power status information on a remote controller using IPMI:

1. Log in as root user.
2. Enter the show ipmi host power command.

   root@host>**show ipmi host** *host* **user** *user* **power**

   - host—IP address of remote host IPMI interface
   - user—IPMI username configured in the remote host

   For example:

   root@host>**show ipmi host 10.10.10.30 user johndoe power**

Powering a Controller On and Off Using IPMI

You can power on or off, and reset a C-series Controller you are currently logged in to and for a remote controller. You must be logged on as a root user.

To execute a power command in the local controller using IPMI:

1. Log in as root user.

   SRC-PE Release 3.1 [R.3.1.0-12]
   login: **root**

2. Enter the password.

   Password: **password**
   — SRC CLI 3.1 build CLI.R.3.1.0.012
   (c) 2005-2008 Juniper Networks Inc.
   root@host>

   You are now logged in as root user.

3. Enter the request ipmi power command.

   user@host>**request ipmi power** (**on** | **off** | **soft-off** | **reset**| **cycle**)

   - on—Power on a C-series Controller
   - off—Power off a C-series Controller. This command does not initiate a clean shutdown of the operating system before powering off the system.
   - soft-off—Power off a C-series Controller softly. This command initiates a soft shutdown of the operating system before powering off the system.
   - reset—Perform a hard reset on a C-series Controller.
   - cycle—Power off and then power on a C-series Controller.

   For example:

   user@host>**request ipmi power off**

To execute a power command on a remote controller using IPMI:

1. Log in as root user.
2. Enter the request ipmi host user power command.

   root@host>**request ipmi host** *host* **user** *user* **power** (**on** | **off** | **soft-off** | **reset**| **cycle**)

   For example:

   root@host>**request ipmi host 10.10.10.30 user johndoe power reset**

Viewing IPMI User Accounts

To display the IPMI user accounts:

- From configuration mode, enter the show command to display all IPMI user accounts.

```
[edit system ipmi]
admin@gnome# show
address 10.227.1.145/24;
gateway 10.227.7.1;
user admin {
   encrypted-password ********;
}
user jdoe {
   encrypted-password ********;
}
```

Creating IPMI User Accounts

An IPMI username and password are required to connect to a remote IPMI interface. You can define new IPMI user accounts using the CLI.

To create an IPMI user account:

1. From configuration mode, access the configuration statement that configures an IPMI interface.

   ```
   user@host# edit system ipmi
   ```

2. Set a plain-text password that is autoencrypted by the CLI.

   ```
   [edit system ipmi]
   user@host# set user name plain-text-password
   ```

   For example:

   ```
   user@host#set user johndoe plain-text password
   New password: xyz123 (text will not appear)
   Re-type new password: xyz123 (text will not appear)
   ```

3. Verify the configuration.

   ```
   [edit system ipmi]
   admin@gnome# show
   address 10.227.1.145/24;
   gateway 10.227.7.1;
   user admin {
      encrypted-password ********;
   }
   user jdoe {
      encrypted-password ********;
   }
   ```

Connecting to a Serial Console Using IPMI Serial over LAN (SOL)

IPMI SOL enables a remote user to monitor and manage a C-series Controller through a serial console by means of an IPMI session. IPMI SOL redirects the C-series Controller's serial port input and output over IP. To connect to a remote serial console using IPMI SOL, the remote system must have IPMI configured. Only one IPMI SOL connection is allowed per IPMI interface.

To connect to a serial host using IPMI SOL:

- From operational mode, enter the ipmisol open command to connect to a serial console.

  user@host>**ipmisol open host *host* user *user***

  - host—IP address of remote host IPMI interface
  - user—IPMI user name configured in the remote host

  For example:

  user@host>**ipmisol open host 10.10.10.30 user johndoe**

To exit from the current IPMI SOL session, enter ~.

Disconnecting from a Serial Console Using IPMI Serial over LAN (SOL)

Only one IPMI SOL connection is allowed per IPMI interface. You can close the active IPMI connection to a local host or to a remote host.

To disconnect from a local host using IPMI SOL:

- From operational mode, enter the ipmisol close local-session command to close the active IPMI connection to a local host.

  user@host>**ipmisol close local-session host**

To disconnect from a remote host using IPMI SOL:

- From operational mode, enter the ipmisol close remote-session command to close the active IPMI connection to a remote host.

  user@host>**ipmisol close remote-session host *host* user *user***

  - host—IP address of remote host IPMI interface
  - user—IPMI user name configured in the remote host

  For example:

  user@host>**ipmisol close remote-session host 10.10.10.30 user johndoe**

Chapter 10

Configuring IPMI on a C-series Platform (C-Web Interface)

This chapter describes how to configure IPMI on a C-series platform with the C-Web interface. Topics include:

Overview of IPMI

Intelligent Platform Management Interface (IPMI) is a message-based hardware management interface that enables remote monitoring, management, and recovery capabilities, regardless of the status of the server. It defines a set of interfaces that are common to computer hardware and firmware that you can use to monitor system health and manage the system.

IPMI operates independently of the operating system (OS) and allows you to manage a system remotely even in the absence of the OS or the system management software, or even if the monitored system is not powered on. IPMI can also function when the OS has started.

IPMI version 1.5 and later can send out alerts by means of a direct serial connection, a LAN, or a serial over LAN (SOL) connection to a remote client. You can then query controller status, review hardware logs, or issue other requests from a remote console through the same connections.

Configuring IPMI with the C-Web Interface

For the C2000 model, an IPMI configuration includes an IP address assigned to the IPMI interface and a gateway IP address. For the C4000 model, only a gateway IP address is required because the IP address for the IPMI interface is the same as the IP address assigned to the eth0 interface on the C4000 model.

To configure IPMI on an interface:

1. Click **Configure**, expand **System**, and then click **IPMI**.

   The IPMI pane appears.

2. In the Address box, enter an IP address.

   - An IP address is required for a C2000 model but is set automatically to the address of the eth0 interface on a C4000 model.
   - address is in the format IP address/destination prefix, such as 10.227.7.145/24.

3. In the Gateway box, enter the default gateway IP address.

   A default gateway is a node on a network that serves as an access point to another network.

4. Click **Apply**.

   The IPMI pane displays the new attributes.

Viewing IPMI User Accounts with the C-Web Interface

To display the IPMI user accounts:

- Click **Configure**, expand **System**, and then click **IPMI > User**.

  IPMI user accounts are listed in the main pane.

Creating an IPMI User Account with the C-Web Interface

An IPMI username and password are required to connect to an IPMI interface. You can create new IPMI user accounts so that IPMI authentication can occur.

To create an IPMI user account:

1. Click **Configure**, expand **System**, and then click **IPMI**.

   The IPMI pane appears.

2. Select **User** from the drop-down list, enter the name of the user in the pop-up dialog box, and click **OK**.

   The IPMI / User pane appears.

3. Enter a password. When the user account is created, the password is encrypted with a Base64 encoding scheme.

4. Click **Apply**.

   The IPMI user appears in the side pane under IPMI.

Deleting an IPMI User Account with the C-Web Interface

To delete an IPMI user account:

1. Click **Configure**, expand **System**, and then click **IPMI**.
2. In the side pane under IPMI, select the user account you want to delete.

   The IPMI / User: (username) pane appears.
3. Click the user account and then click **Delete** in the IPMI / User: (username) pane.

   The user account is deleted.

Renaming an IPMI User Account with the C-Web Interface

To rename an IPMI user account:

1. Click **Configure**, expand **System**, and then click **IPMI**.
2. In the navigation tree under IPMI, select the user account you want to rename.

   The IPMI / User: (username) pane appears.
3. Click the user account and then click **Rename** in the IPMI / User: (username) pane.

   The user account is deleted.
4. Type a new name and click **OK**.

   The user account is renamed.

Chapter 11

Installation Guidelines and Requirements

This chapter reviews preinstallation considerations such as electrical, environmental, and safety compliances for the C-series Controllers. For complete system specifications, see “System Specifications” on page 35. Topics include:

Your Preinstallation Responsibilities

Complete the following tasks before installing the system:

- Verify that the electrical supply meets all AC and DC power requirements. See “System Specifications” on page 35.
- Verify that the site meets all environment specifications. See “Environmental Requirements” on page 55 and “System Specifications” on page 35.
- Verify that the cables you plan to use meet the specifications, and review the cabling recommendations. See “Cabling Recommendations” on page 60.
- Verify the operation of all telephone circuits, digital services, and T1 facilities required for installation.
- Ensure that all IP requirements are met, such as IP addresses, subnet masks, and any specific routing protocol information.

Environmental Requirements

See “System Specifications” on page 35 for complete environmental specifications.

Choose a location for the system that is dry, relatively dust free, well ventilated, and air conditioned. If you install equipment in a rack, be sure that the floor is capable of supporting the combined weight of the rack and the installed equipment. Place the system in a location with sufficient access to power and network cables.

Like other network devices, the system generates a significant amount of heat. You must provide a balanced environment so that the system performs properly and safely. See “System Specifications” on page 35 for acceptable ranges of temperature and humidity.

Be sure to allow enough space around the system for adequate ventilation. Inadequate ventilation can cause the system to overheat.

CAUTION: Do not block the air vents on the system. Otherwise, the system might overheat.

Regulatory Compliances

See “System Specifications” on page 35 for a complete list of regulatory compliance requirements, including safety, EMC, and telecommunications.

Safety Notices

For your safety, before installing the system, review all safety notices in this topic.

Lithium Battery

WARNING: There is a danger of explosion if the battery is incorrectly replaced. Return the device to the manufacturer for battery replacement. Moreover, never open the chassis under any circumstances. Doing so will also void the warranty.

WARNING: La batterie présente un risque d’explosion si elle n’est pas remplacée comme il se doit. Retournez l’appareil au fabricant pour faire remplacer la batterie. Le châssis ne doit par ailleurs en aucun cas être ouvert. Cela annulerait la garantie.

Power Disconnection

WARNING: Before working on a device that has an On/Off switch, turn the power off and disconnect the power cord to all power supplies.

For DC power supplies, 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.

WARNING: Avant de commencer à travailler sur un appareil muni d'un interrupteur On. Off (Marche/Arrêt), Coupez l'alimentation et débranchez le cordon d'alimentation de toute source d'alimentation.

Dans le cas d'une alimentation à courant continu, repérez le disjoncteur sur le tableau de contrôle qui alimente le circuit c.c., placez-le en position d'off (arrêt) et maintenez le bouton du disjoncteur en position d'arrêt à l'aide de ruban adhésif.

Power Cable Warning

WARNING: This unit has two power cables. To avoid electric shock, disconnect both power cables before servicing the unit.

WARNING: Cette unité possède deux cordons d'alimentation. Pour supprimer tout risque électrique, débranchez les deux cordons d'alimentation de l'unité.

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。

Working with Lasers

Some Juniper Networks devices are equipped with fiber-optic ports, which emit radiation that may be harmful to the human eye. Fiber-optic ports are considered Class 1 laser or Class 1 LED ports.

WARNING: Class 1 Laser product.

WARNING: Class 1 LED product.

WARNING: Do not stare into the laser beam or view it directly with optical instruments.

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation might be emitted from the aperture of the port when no fiber cable is connected.

These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

VCCI Compliance

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. (VCCI-A)

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Ａ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Safety Guidelines

For your safety, before installing the system, review all safety warnings in this topic.

WARNING: The recommended maximum ambient temperature is 40°° C (104° F). For safe operation take into consideration the internal temperature within the rack.

WARNING: Install equipment in the rack from the bottom upward. Doing this helps maintain the stability of the rack and reduces the chance of the rack tipping over.

WARNING: Do not insert any metal object, such as a screwdriver, into the system. Doing so can cause electric shock and serious burns.

WARNING: Three people are required to install the system in a rack: two to lift the system into position and one to screw it to the rack.

WARNING: Connect the system or rack to ground (earth), and ensure that a reliable grounding path is maintained in the rack.

WARNING: Do not work on the system or connect or disconnect cables during lightning activity.

WARNING: Be sure that circuit breakers for the power source are in the OFF position before attaching power cables.

WARNING: Before servicing the system, turn off the power.

WARNING: Remove jewelry (including rings, necklaces, and watches) before working on equipment that is connected to power lines. Metal objects heat up when connected to power and ground and can cause serious burns or become welded to the terminals.

CAUTION: Evaluate the overall loading of the branch circuit before you install any equipment into a rack.

Equipment Rack Requirements

When allocating equipment rack space, consider the following:

- Type of equipment racks recommended for the system
- Number of equipment racks required to hold your current system configuration
- Future expansion

Make sure that your distribution rack meets basic mechanical and space requirements and complies with conventional standards. In the United States, use the EIA-310-D Cabinets, Racks, Panels, and Associated Equipment, September 1992 standard.

Mechanical Requirements

Follow these mechanical requirements for your rack:

- Select from the following rack options:
  - Two-post rack—A freestanding enclosed cabinet with two mounting posts in the front
  - Telco-type rack—Two adjacent mounting posts that you must secure to the floor or an overhead structure
  - Four-post rack—A freestanding open rack, either open or closed
- The rack must have at least two mounting posts.
- The distance between the mounting holes in the two posts must be 18.31 inches ± .063 inch, as specified in EIA-310-D.
- An optional mounting kit is available for midchassis mounting. Contact your Juniper Networks sales representative for more information.

Space Requirements

If you use an enclosed rack for the system, ensure that there is a minimum of 3 inches of clearance between the inner side wall and the system. This clearance space ensures adequate air flow.

Proper Rack Installation

To confirm proper equipment rack installation, verify the following:

- Racks are installed and electrically grounded according to manufacturer instructions.
- Equipment racks are anchored to the floor and, when possible, anchored to the ceiling as well.
- Equipment rack installations comply with applicable local, state, and national codes.

Cabling Recommendations

Comply with the following recommendations:

- Use only shielded cables.
- Ensure that cable distance and rate limits meet IEEE-recommended maximum distances and speeds for signaling purposes. For information about attenuation and power loss in optical fiber cables see:
  - ANSI T1.646a-1997 Telecommunications – Broadband ISDN - Physical Layer Specification for User-Network Interfaces Including DS1/ATM (1997)
  - ANSI T1.646-1995 Telecommunications – Broadband ISDN - Physical Layer Specification for User-Network Interfaces Including DS1/ATM (1995)
- Ensure that power cables deliver sufficient power to the system.
- Attach laser fiber connectors only to Class 1 laser devices in accordance with IEC 60825-1, Safety of Laser Products - Part 1.

- Route cables so that they do not restrict ventilation or airflow.
- Route cables so that modules and field-replaceable units are easily accessible.
- Route cables in a logical direction to prevent loss of connectivity to other equipment in the rack, to associated equipment in adjacent racks, or to the backbone network.

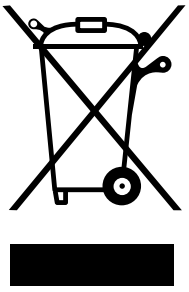
For additional cable recommendations, consult the document GR-63–CORE: Network Equipment Building System (NEBS) Requirements: Physical Protection, Issue 2, April 2002.

Product Reclamation and Recycling Program

Juniper Networks is committed to environmentally responsible behavior. As part of this commitment, we continually work to comply with environmental standards such as the European Union's *Waste Electrical and Electronic Equipment* (WEEE) Directive and *Restriction of Hazardous Substances* (RoHS) Directive.

These directives and other similar regulations from countries outside the European Union regulate electronic waste management and the reduction or elimination of specific hazardous materials in electronic products. The WEEE Directive requires electrical and electronics manufacturers to provide mechanisms for the recycling and reuse of their products. The RoHS Directive restricts the use of certain substances that are commonly found in electronic products today. Restricted substances include heavy metals, including lead, and polybrominated materials. The RoHS Directive, with some exemptions, applies to all electrical and electronic equipment.

In accordance with Article 11(2) of Directive 2002/96/EC (WEEE), products put on the market after 13 August 2005 are marked with the following symbol or include it in their documentation: a crossed-out wheeled waste bin with a bar beneath.



Juniper Networks provides recycling support for our equipment worldwide to comply with the WEEE Directive. For recycling information, go to http://www.juniper.net/environmental, and indicate the type of Juniper Networks equipment that you wish to dispose of and the country where it is currently located, or contact your Juniper Networks account representative.

Products returned through our reclamation process are recycled, recovered, or disposed of in a responsible manner. Our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

Hardware Compliance

C–series Controllers meet the hardware compliance requirements in this topic.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A 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.

This equipment is designed for use with properly shielded and terminated cables. Refer to the installation sections of this manual before operation.

Reference: CFR 47, Part 15J, Sect 15.105 April 18, 1989

Caution: Changes or Modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Requirements for Consumer Products

This equipment complies with FCC rules, Part 68. On the back side of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. If requested, provide this information to your telephone company.

If this equipment causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be given advance notice so as to give you an opportunity to maintain uninterrupted service.

If you experience trouble with this equipment, please contact the manufacturer for warranty/repair information. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

Food and Drug Administration, Center for Devices and Radiological Health

This equipment complies with 21 CFR 1040.10 and 1040.11 for the safe use of lasers.

Canadian Department of Communications Radio Interference Regulations

This Class B (or Class A, if so indicated on the registration label) digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Réglement sur le brouillage radioélectrique du ministère des communications

Cet appareil numérique de la Classe B (ou Classe A, si ainsi indiqué sur l'étiquette d'enregistration) respecte toutes les exigences du Reglement sur le Materiel Brouilleur du Canada.

Industry Canada Notice CS-03

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's 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 and acceptable method of connection. 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 coordinated by a representative 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.

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.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Avis CS-03 d'Industrie Canada

L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur. Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par lefournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement del'appareillage, le service de télécommunications peut demander le débranchment de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Avis: Veuillez prendre note que pour tout appareillage supportant des lignes de type “loopstart,” l'indice d'équivalence de la sonnerie (IES) assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface. La terminaison d'une interface téléphonique peut consister en une combinaison de quelques dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5. Le REN figure sur l'étiquette “FCC Rules Part 68” située sur le support du module ou à l'arrière de l'unité.

D.O.C. Explanatory Notes: Equipment Attachment Limitations

The Canadian Department of Communications label identifies certified equipment. This certification meets certain telecommunication network protective, operational and safety requirements. The department does not guarantee the equipment will operate to the users satisfaction.

Before installing the 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 company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition 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.

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.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Notes explicatives du ministère des Communications: limites visant les accessoires

L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d'un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchment de l'appareillage.

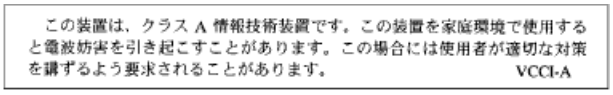
Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

EC Declaration of Conformity

The EC Declaration of Conformity is available in “Declaration of Conformity” on page 71.

Voluntary Control Council for Interference (VCCI) Statement for Japan


この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

The preceding translates as:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. VCCI-A

Chapter 12

Contacting Customer Support and Returning Hardware

See the Juniper Networks Web site for complete customer service information:

- http://www.juniper.net/support/guidelines.html

Topics in this chapter include:

Contacting Customer Support

For your convenience, we provide multiple options for requesting and receiving technical support from the Juniper Networks Technical Assistance Center (JTAC):

- By the Web using Juniper Networks, Inc. Case Manager:

  https://www.juniper.net/cm/index.jsp

- By telephone:
  - From the US, Canada, and Mexico at 1–888–314–JTAC
  - From all other locations at 408–745–9500

Return Procedure

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 68.
2. Obtain a Return Materials Authorization (RMA) number from the JTAC. See “Information You Might Need to Supply to JTAC” on page 68.

Provide the following information in your e-mail message or during the telephone call:

- Part number and serial number of the component
- Your name, organization name, telephone number, and fax number
- Shipping address for the replacement component, including contact name and phone number
- Description of the failure

The support representative validates your request and issues an RMA number for return of the component.

3. Pack the component for shipment, performing the procedure described in "Returning Products for Repair or Replacement" on page 69.

Locating Component Serial Numbers

Before contacting Juniper Networks to request a RMA, you must find the serial number on the chassis or component. To list all the chassis components and their serial numbers, enter the following command:

```
user@host>show system information
```

You can also find the serial numbers on the components.

Information You Might Need to Supply to JTAC

When requesting technical support from JTAC by phone, be prepared to provide the following information:

- Priority level
- Indication of what activity was being performed on the system when the problem occurred
- Problem detail and configuration data, obtained by this command:
  - show configuration
  - show system configuration

When a new request for technical support is submitted, the JTAC engineer:

1. Opens a case and assigns a number.
2. Begins troubleshooting, diagnostics, and problem replication (if appropriate).
3. Provides you with periodic updates on problem status and escalates the problem as appropriate according to escalation management guidelines.
4. Closes the case when you agree that the problem has been resolved.

Tools and Parts Required

To remove components from the chassis or the chassis from a rack before you return the chassis or components for repair or replacement, you need the following tools and parts:

- Mechanical lift, if available
- 3/8–inch wrench or nut driver
- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding device
- Flat-blade (—) screwdriver
- Phillips (+) screwdrivers, numbers 1 and 2
- Plastic boots or other protective cover for fiber-optic connectors
- Wire cutters

Returning Products for Repair or Replacement

In the event of a hardware failure, please contact Juniper Networks to obtain a Return Material Authorization (RMA) number. This number is necessary to ensure proper tracking and handling of returned material at the factory. Do not return any hardware until you have received an RMA. Juniper Networks reserves the right to refuse shipments that do not have an RMA. Refused shipments are returned to the shipper via collect freight.

Packing Instructions for Returning a Chassis

If possible, use the original shipping crate, pallet, and packing materials in which the chassis was originally shipped. If these materials are unavailable, use comparable shipping material, or contact your Juniper Networks representative for information on approved packaging material.

To pack the chassis for shipment:

1. Ground yourself by using an antistatic wrist strap or other device.
2. Issue the proper shutdown commands to halt your system.
3. Power the system down by pressing the PWR button.
4. Remove all cables from the chassis.
5. Remove the chassis from the rack.
6. Pack the chassis securely in a proper shipping container, covering the chassis with an ESD bag and placing packing foam on top of and around the chassis.

Chapter 13

Declaration of Conformity

This chapter contains the following topics:

Declaration of Conformity – C2000 Controller

Declaration of Conformity
Juniper Networks, Inc. 10 Technology Park Drive Westford, Massachusetts 01886 USA declares that under our sole responsibility the product(s) **Server** **Model C2000** is in conformity with the provisions of the following EC Directives, including all amendments, and with national legislation implementing these directives: **Low Voltage Directive 73/23/EEC** **EMC Directive 89/336/EEC** and that the following harmonized standards have been applied: EN 60950-1:2000 + A11 EN 60825-1:1994 + A1 + A2 EN 300 386 V1.3.3:2005 EN 55024:1998 + A1 + A2 EN 55022:1998 + A1 (2000) + A2 (2003) Class A

Place	Signature	Date
Westford, MA	Susanne Delisle	07/24/2007

Declaration of Conformity – C4000 Controller

Declaration of Conformity

Juniper Networks, Inc.
10 Technology Park Drive
Westford, Massachusetts 01886 USA

declares that under our sole responsibility the product(s)

Server
Model C4000

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

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

and that the following harmonized standards have been applied:

EN 60950-1:2000 + A11
EN 60825-1:1994 + A1 + A2
EN 55024:1998 + A1 + A2
EN 61000-3-2, EN 61000-3-3
EN 55022:1998 + A1 (2000) + A2 (2003) Class A

Place	Signature	Date
Westford, MA	Susanne Delisle	07/24/2007

Part 4
Index

■ Index on page 75

Index