JUNOS™
Internet Software
for M-series and T-series Routing Platforms

Network Operations Guide

Hardware

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-012090-01, Revision 1

JUNOS Internet Software for M-series and T-series Routing Platforms Network Operations Guide: Hardware

Writer: Donice G. Mitchell
Editor: Sonia Saruba
Covers and template design: Edmonds Design

Thanks to Damien Halloway, Jim Boyle, John Hammond, John Jacobs, Majid Ansari, Nitin Serro, Richard Southerland, and Robert Kim for their help with the revision of this guide.

Revision History
21 March 2005—Revision 1

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

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

Year 2000 Notice

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

Software License

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

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

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

End User License Agreement

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

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

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

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

a. Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.

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.

c. Other Juniper documentation for the Software (such as product purchase documents, documents accompanying the product, the Software user manual(s), Juniper's website for the Software, or messages displayed by the Software) may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, concurrent users, sessions, subscribers, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, or capabilities, or provide temporal or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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, 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; (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, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) 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.

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. If the Software is distributed on physical media (such as CD), Juniper warrants for 90 days from delivery that the media on which the Software is delivered will be free of defects in material and workmanship under normal use. This limited warranty extends only to the Customer. Except as may be expressly provided in separate documentation from Juniper, no other warranties apply to the Software, and the Software is otherwise provided AS IS. Customer assumes all risks arising from use of the Software. Customer's sole remedy and Juniper's entire liability under this limited warranty is that Juniper, at its option, will repair or replace the media containing the Software, or provide a refund, provided that Customer makes a proper warranty claim to Juniper, in writing, within the warranty period. Nothing in this Agreement shall give rise to any obligation to support the Software. Any such support shall be governed by a separate, written agreement. To the maximum extent permitted by law, Juniper shall not be liable for any liability for 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 HEREIN OR IN SEPARATE DOCUMENTATION PROVIDED FROM JUNIPER AND 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.

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

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

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to you may contain encryption or other capabilities restricting your 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. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. 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.

If you have any questions about this agreement, contact Juniper Networks at the following address:

■

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Attn: Contracts Administrator

Abbreviated Table of Contents

Table of Contents

Part 3 Monitoring Key and Common Router Components

Chapter 12 Monitoring Key Router Components 91

Chapter 13 Monitoring the Router Chassis 107

Chapter 14 Monitoring the Routing Engine 125

Part 5 Monitoring M40e and M160 Internet Router-Specific Components

Chapter 28 Monitoring the PCG 369

Chapter 29 Monitoring the CIP 381

Part 6 Monitoring M40 Internet Router-Specific Components

Chapter 30 Monitoring the SCB 393

Part 7 Monitoring M20 Internet Router-Specific Components

Chapter 31 Monitoring the SSB 405

Part 8 Monitoring M7i and M10i Router-Specific Components

Part 9 Monitoring M5 and M10 Router-Specific Components

Part 10 Monitoring Redundant Router Components

Part 11 Appendices

Part 12 Index

About This Manual

This chapter provides a high-level overview of the *JUNOS Internet Software for M-series and T-series Routing Platforms Hardware Network Operations Guide*:

Objectives

This manual provides operational information helpful in monitoring Juniper Networks M-series and T-series router components and isolating potential problems. This manual is not directly related to any particular release of the JUNOS Internet software.

To obtain the most current version of this manual, refer to the product documentation page on the Juniper Networks Web site, which is located at http://www.juniper.net/.

Audience

This manual is designed for Network Operations Center (NOC) personnel who monitor a Juniper Networks router.

It assumes that you have a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. This manual assumes that you are familiar with one or more of the following Internet routing protocols: Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Internet Control Message Protocol (ICMP) router discovery, Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), Protocol-Independent Multicast (PIM), Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), and Simple Network Management Protocol (SNMP).

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

Document Organization

This manual is divided into several parts. Each part describes the most common tasks for monitoring a particular interface, and the individual chapters within a part describe one or more step-by-step procedures for each task.

This manual also contains a complete index.

Chapter Organization

Most chapters in this manual consist of a checklist at the beginning of the chapter listing the tasks and commands for monitoring the component. The tasks and commands are then explained in step-by-step procedures.

Each step-by-step procedure consists of some or all of the following parts:

- Purpose—Describes what is affected if this task is not performed or what is accomplished with this task.
- What Is... —Describes a component (usually hardware).
- Step(s) To Take—Lists the steps in the task.
- Action—Describes an action to perform in order to complete the step.
- Sample Output—Presents sample output relevant to the procedure.
- What It Means—Describes or summarizes what is presented in the sample output.
- Symptom/Indications—Describes a problem with the software or hardware.
- See Also—Lists other topics related to this task.
- Alternative Actions—Describes other commands or ways of doing the task.

- Syntax—Describes the full syntax of the command or configuration statement. For an explanation of how to read the syntax statements, see “Documentation Conventions” on page xxix.

Documentation Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

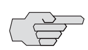
Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.

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

Table 2: Text and Syntax Conventions

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

Convention	Element	Example

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

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

Related Juniper Networks Documentation

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

Table 3: Juniper Networks Technical Documentation

Document	Description
JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms Configuration Guides	
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
JUNOS-FIPS Configuration Guide	(M-series and T-series routing platforms only) Provides an overview of JUNOS-FIPS 140-2 concepts and describes how to install and configure the JUNOS-FIPS software. Describes FIPS-related commands and how to configure, authorize, and zeroize the AS II FIPS PIC.
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
Multicast Protocols	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
Network Interfaces and Class of Service	Provides an overview of the network interface and class-of-service functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
Network Management	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, forwarding options, and cflowd.
Routing Protocols	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.

Document	Description
System Basics	Provides an overview of the JUNOS software and describes how to install and upgrade the software. This guide also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.
VPNs	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
Network and Services Interfaces Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot network and services interfaces on Juniper Networks J-series, M-series, and T-series routing platforms.
Protocols, Class of Service, and System Basics Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot most aspects of Juniper Networks J-series, M-series, and T-series routing platforms.
System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
JUNOScript API Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
JUNOScript API Configuration Reference	Provides a reference page for the configuration tags in the JUNOScript API.
JUNOScript API Operational Reference	Provides a reference page for the operational tags in the JUNOScript API.
JUNOS Comprehensive Index and Glossary	
Comprehensive Index and Glossary	Provides a complete index of all JUNOS software books and the *JUNOScript API Guide*. Also provides a comprehensive glossary.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
J-series Services Router Documentation	
J-series Services Router Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity.
J-series Services Router Configuration Guide	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols. The guide also shows how to configure virtual private networks (VPNs), configure and manage multicast networks, and apply routing techniques such as policies, firewall filters, IP Security (IPSec) tunnels, and service classification for safer, more efficient routing.
J-series Services Router Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
M-series and T-series Hardware Documentation	
Hardware Guide	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
PIC Guide	Describes the routing platform Physical Interface Cards (PICs). Each platform has its own PIC guide.

Document	Description
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS and JUNOScript manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
Hardware Release Notes	Describe the available documentation for the routing platform and the supported PICs, and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
JUNOScope Software Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
J-series Services Router Release Notes	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 4: JUNOS Internet Software Network Operations Guides

Book	Description
JUNOS Internet Software for M-series and T-series Routing Platforms Network Operations Guides	
Baseline	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
Interfaces	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
MPLS	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
Hardware	Describes tasks for monitoring M-series and T-series routing platforms.

Documentation Feedback

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

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

Requesting Support

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

Part 1
Understanding M-series and T-series Internet Routers

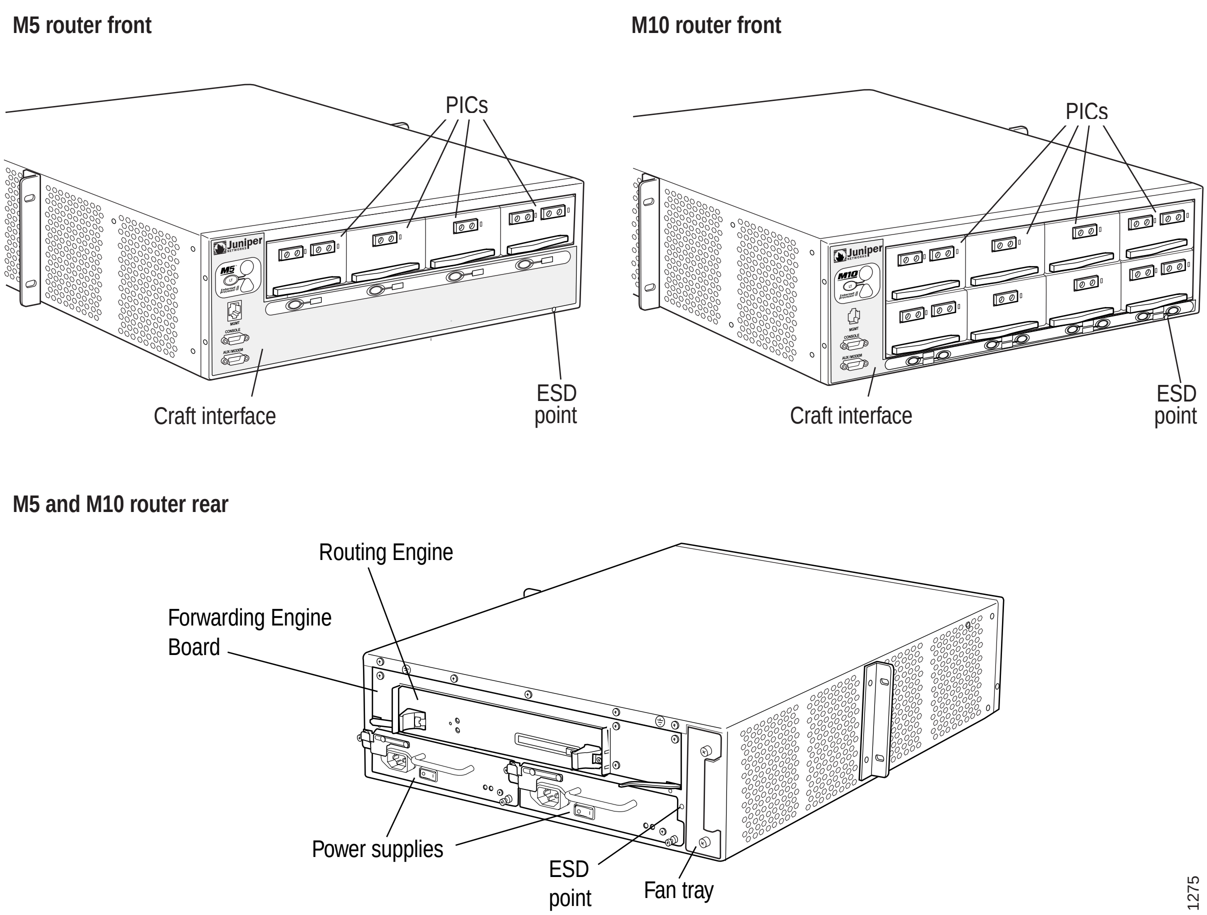
Chapter 1

M5 and M10 Internet Router Overview

NOTE: See the End-of-sale and End-of-service Announcement for the M5 and M10 routing platforms and products at https://www.juniper.net/support/eol/.

The M5 and M10 Internet routers provide edge and core applications for small IP networks where space and power are at a premium. The routers support the JUNOS software which provides router configuration and monitoring. (See Figure 1.)

Figure 1: M5 and M10 Routers



The M5 and M10 routers include the router-specific Forwarding Engine Board (FEB) component that provides route lookup, filtering, and sampling, as well as switching to the destination Physical Interface Card (PIC). The FEB performs the function of the Flexible PIC Concentrators (FPCs) on other M-series routers. The FEB contains the Internet Processor II application-specific integrated circuit (ASIC), two distributed Buffer Manager ASICs, and two I/O Manager ASICs, and is responsible for making forwarding decisions, distributing packets throughout memory, and forwarding notification of outgoing packets.

The M5 and M10 routers provide a wide range of high-performance interfaces from T1 and E1 through OC12c/STM4 (for the M5 router) or OC48c/STM16 (for the M10 router). PICs between the two routers are interchangeable. For more information about supported PICs and FPCs for each M-series router type, see the appropriate PIC installation guide.

The M5 and M10 router Internet processor II ASIC forwards packets at a throughput rate of up to 5 Gbps for the M5 router and up to 10 plus Gbps for the M10 router. The ASIC technology provides such packet processing as rate limiting, filtering, and sampling of IP services.

M5 and M10 Router Components

Table 5 lists the major M5 and M10 router components and characteristics.

Table 5: M5 and M10 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Cooling system	1 fan tray (3 fans)	Cools router components	Yes	Hot-removable, hot-insertable	–
Craft interface	1	Displays the status and allows you to perform control functions	–	–	–
FEB	1	Connects PICs to other components and houses shared memory	–	Requires router shutdown	–
PIC	1–4 M5 routers 1–8 M10 routers	Provides interfaces to various network media	–	Hot-removable, hot-insertable	Yes
Power supply	2 AC or 2 DC	Distributes needed voltages to components	Yes	Hot-removable, hot-insertable	–
Routing Engine	1	Handles routing protocols and maintains routing tables	–	Requires router shutdown	–

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M5 and M10 Router Components

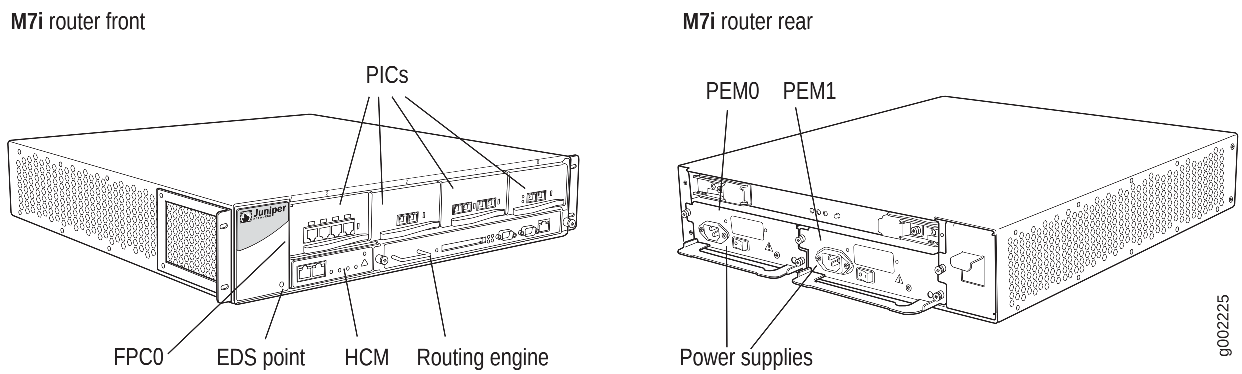
See the following chapters for information about monitoring the M5 and M10 router components:

- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring PICs” on page 183
- “Monitoring the Craft Interface” on page 197
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507
- “Monitoring the Cooling System” on page 251
- “Monitoring Redundant Cooling System Components” on page 523
- “Maintaining the Cable Management System, Cables, and Connectors” on page 275
- “Monitoring the FEB” on page 453

Chapter 2
M7i Internet Router Overview

The M7i Internet router provides security and performance in small to medium Points of Presence (PoPs), as well as a carrier-class customer premise equipment (CPE) solution for managed services and campus border router applications. (See Figure 2.)

Figure 2: M7i Router



The M7i router includes the Compact Forwarding Engine Board (CFEB) which provides route lookup, filtering, and switching on incoming data packets, then directs outbound packets to the appropriate interface for transmission to the network. It can process 16 million packets per second (Mpps). The CFEB communicates with the Routing Engine using a dedicated 100-Mbps link that transfers routing table data from the Routing Engine to the forwarding table. The link is also used to transfer routing link-state updates and other packets destined for the router from the CFEB to the Routing Engine.

A built-in tunnel interface encapsulates arbitrary packets inside a transport protocol, providing a private, secure path through an otherwise public network. The built-in tunnel interface on the CFEB is configured the same way as a PIC. For information about configuring the built-in tunnel interface, see the *JUNOS Services Interfaces Configuration Guide*.

The Adaptive Services PIC-Integrated (ASP-I) is an optional component on the CFEB which performs one or more services on traffic—Stateful firewall, Network Address Translation (NAT) or intrusion detection services (IDS)—before it reaches its destination.

In addition to accommodating up to four Physical Interface Cards (PICs), the M7i router includes a built-in Fixed Interface Card (FIC) that provides two Fast Ethernet ports or one Gigabit Ethernet port, depending on which FIC or which model was ordered. For more information about Fast Ethernet and Gigabit Ethernet interfaces, see the *M7i Internet Router PIC Guide*.

The M7i router supports various PICs, including ATM, channelized, Ethernet, IP services, and SONET/SDH interfaces. For more information about supported PICs, see the *M7i Internet Router PIC Guide*.

The M7i router provides a maximum aggregate throughput of 8.4 gigabits per second (Gbps). Control operations in the router are perform Control operations in the router are performed by the Routing Engine, which runs JUNOS software to handle routing protocols, traffic engineering, policy, policing, monitoring, and configuration management. Forwarding operations in the router are performed by the Packet Forwarding Engine.

M7i Router Components

Table 4 lists the major M7i router components and characteristics.

Table 4: M7i Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
CFEB	1	Provides route lookup, management of shared memory, transfer of outgoing data packets, and transfer of exception and control packets; includes built-in tunnel interface and optional Adaptive Services PIC	–	Hot-pluggable (routing functions are interrupted when removed)	Yes
Cooling system	1 fan tray (4 fans)	Cools router components	–	Hot-removable, hot-insertable	–
FIC	1	Receives incoming packets and transmits outgoing packets to the network, displays alarm status, and takes PICs online and offline (2 Fast Ethernet or 1 Gigabit Ethernet)	–	Built-in	PICs On/Off button
PIC	1–4	Provides interfaces to various network media and performs framing and line-speed signaling	–	Hot-removable, hot-insertable	Yes
Power supply	2 AC or 2 DC	Distributes needed voltages to components	Yes	Hot-removable, hot-insertable	Yes
Routing Engine	1	Maintains the routing tables, manages the routing protocols, controls the interfaces, controls some chassis components, and provides the interface for system management and user access	–	Hot-pluggable (routing functions are interrupted when removed)	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M7i Router Components

See the following chapters for information about monitoring the M7i router components:

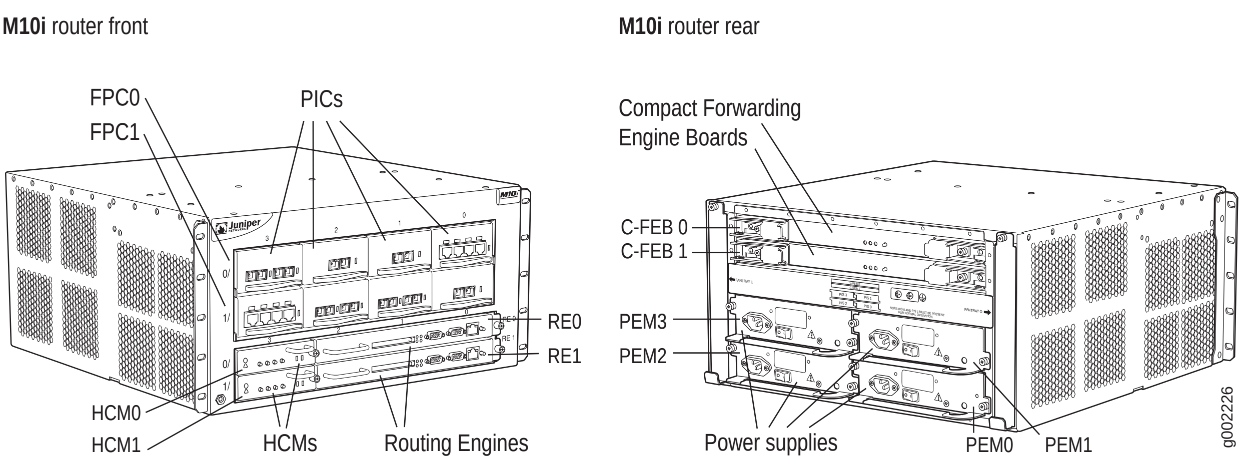
- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring PICs” on page 183
- “Monitoring the FIC” on page 443
- “Monitoring the CFEBs” on page 417
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507
- “Monitoring the Cooling System” on page 251

Chapter 3

M10i Internet Router Overview

The M10i Internet router provides high-speed interfaces for medium and large networks and network applications, such as those supported by Internet service providers (ISPs). (See Figure 3.)

Figure 3: M10i Router



The M10i router includes the router-specific Compact Forwarding Engine Board (CFEB) which performs route lookup, filtering, and switching on incoming data packets, then directs outbound packets to the appropriate Flexible PIC Concentrator (FPC) for transmission to the network. It can process 16 million packets per second (Mpps).

A High-Availability Chassis Manager (HCM) works with its companion Routing Engine to provide control and monitoring functions for router components. The HCM also displays alarm status and takes Physical Interface Cards (PICs) online and offline.

On the M10i router, built-in FPCs house the PICs that connect the router to network media. The router supports up to eight PICs, including ATM, Channelized, Gigabit Ethernet, IP Services, and SONET/SDH interfaces. For more information on PICs, see the *M10i Internet Router PIC Guide*.

Some PICs, such as Gigabit Ethernet PICs, accept small form-factor pluggable tranceivers (SFPs), which are fiber-optic transceivers that can be removed from the PIC.

The M10i router provides a maximum aggregate throughput of 12.8 gigabits per second (Gbps). Control operations in the router are performed by the Routing Engine, which runs JUNOS software to handle routing protocols, traffic engineering, policy, policing, monitoring, and configuration management. Forwarding operations in the router are performed by the Packet Forwarding Engine.

M10i Router Components

Table 5 lists the major M10i router components and characteristics.

Table 5: M10i Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
CFEB	1 or 2	Provides route lookup, filtering, and switching on incoming data packets; directs outbound packets to the appropriate FPC for transmission to the network	Yes	Hot-pluggable	Yes
Cooling system	2 fan trays (8 fans)	Cools router components	Yes	Hot-removable, hot-insertable	–
FPC	2	House the PICs that connect the router to network media	–	Built-in	–
HCM	2	Works with a companion Routing Engine to provide control and monitoring functions for router components; displays alarm status; takes PICs online and offline		Hot-pluggable	–
PIC	1–8	Provides interfaces to various network media; receives incoming packets from the network and transmits outgoing packets to the network, performing framing and line-speed signaling for their media type; encapsulates outgoing packets received from the FPCs before transmitting them.	–	Hot-removable, hot-insertable	Yes (On the HCM)
Power supply	1–4 AC or DC	Distributes needed voltages to components	Yes	Hot-removable, hot-insertable	Yes
SFP		Fiber-optic transceivers that connect to PICs	–	Hot-removable, hot-insertable	–
Routing Engine	1 or 2	Runs the JUNOS software; maintains the routing tables, manages the routing protocols used on the router, controls the router's interfaces, controls some chassis components, and provides the interface for system management and user access to the router	Yes	Hot-pluggable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M10i Router Components

See the following chapters for information about monitoring the M10i router components:

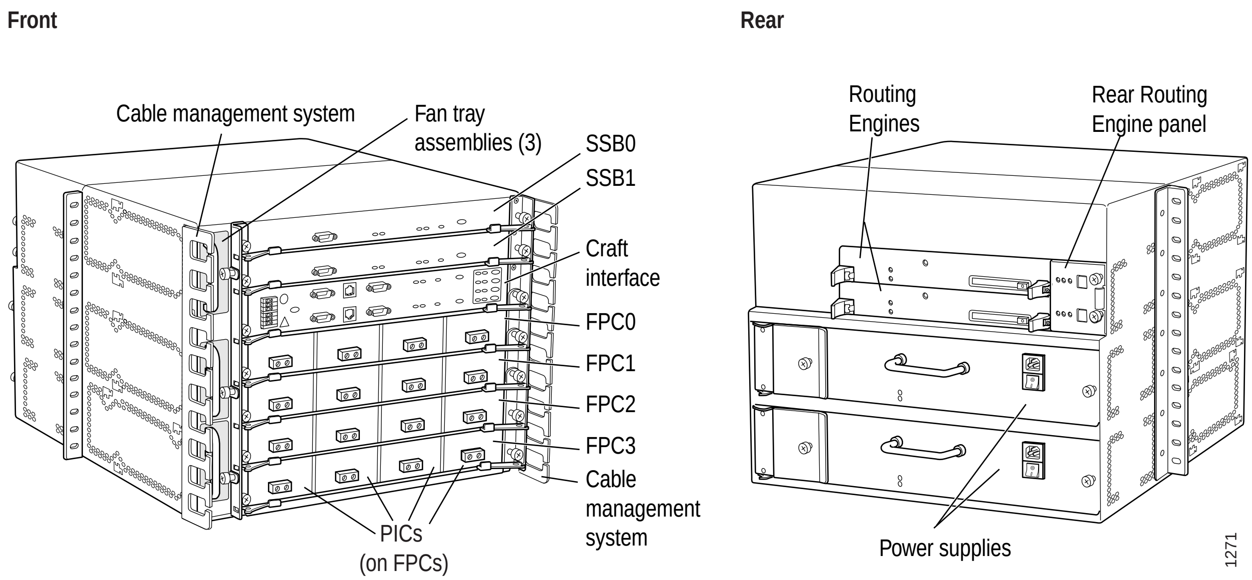
- "Monitoring the Router Chassis" on page 107
- "Monitoring the Routing Engine" on page 125
- "Monitoring FPCs" on page 163
- "Monitoring PICs" on page 183
- "Monitoring the FIC" on page 443
- "Monitoring the CFEBs" on page 417
- "Monitoring the HCM" on page 431
- "Monitoring Power Supplies" on page 217
- "Monitoring Redundant Power Supplies" on page 507
- "Monitoring the Cooling System" on page 251
- "Maintaining the Cable Management System, Cables, and Connectors" on page 275

Chapter 4

M20 Internet Router Overview

The M20 Internet router provides dedicated access, public and private peering, and hosting sites for medium core IP networks. The M20 router supports the JUNOS software which provides router configuration and monitoring. (See Figure 4.)

Figure 4: M20 Router



The M20 router includes the router-specific System and Switch Board (SSB) that provides route lookup, filtering, and sampling to the destination Flexible PIC Concentrator (FPC). The SSB contains both the Internet Processor II application-specific integrated circuit (ASIC) and the Distributed Buffer Manager ASIC, and makes forwarding decisions, distributes data cells throughout memory, processes exception and control packets, monitors system components, and controls FPC resets. You can install up to two SSBs.

Physical Interface Cards (PICs) are available in supported media types, including Asynchronous Transfer Mode (ATM), Channelized, DS3, E1, E3, T1, Ethernet, SONET/SDH, and IP services. The M20 and M40 router FPCs and PICs are interchangeable, and most of the PICs can also be used in the M40e Internet router. For more information about supported PICs and FPCs for each M-series router type, see the appropriate PIC installation guide.

The M20 router Internet Processor II ASIC forwards packets at a throughput rate of up to 20Gigabits per second (Gbps). An optional redundant switching fabric and Routing Engine increase system availability and ensure automatic failover in case of component failure. The ASIC technology provides such packet processing as route lookups, filtering, sampling, rate limiting, load balancing, buffer management, switching, and encapsulation and de-encapsulation of IP services.

M20 Router Components

Table 6 lists the major M20 router components and characteristics.

Table 6: M20 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Cooling system	3 fan trays and 1 rear Routing Engine fan	Cools router components	Yes	Hot-removable, hot-insertable	–
Craft interface	1	Displays the status and allows you to perform control functions	–	Hot-removable, hot-insertable	–
FPC	1–4	Connects PICs to other components and houses shared memory	–	Hot-removable, hot-insertable	Yes
PIC	1–4 per FPC	Provides interfaces to various network media	–	Hot-removable, hot-insertable	–
Power supply	2 AC or 2 DC	Distributes needed voltages to components	Yes	Hot-removable, hot-insertable	–
Routing Engine	1–2	Handles routing protocols and maintains routing tables	Yes	Hot-pluggable	Yes
SSB	1–2	Performs router lookups, manages shared memory, and transfers control packets	Yes	Hot-pluggable	–

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M20 Router Components

See the following chapters for information about monitoring the M20 router components:

- "Monitoring the Router Chassis" on page 107
- "Monitoring the Routing Engine" on page 125
- "Monitoring Redundant Routing Engines" on page 491
- "Monitoring FPCs" on page 163
- "Monitoring PICs" on page 183
- "Monitoring the Craft Interface" on page 197
- "Monitoring Power Supplies" on page 217
- "Monitoring Redundant Power Supplies" on page 507
- "Monitoring the Cooling System" on page 251
- "Monitoring Redundant Cooling System Components" on page 523
- "Maintaining the Cable Management System, Cables, and Connectors" on page 275
- "Monitoring the SSB" on page 405
- "Monitoring Redundant SSBs" on page 605

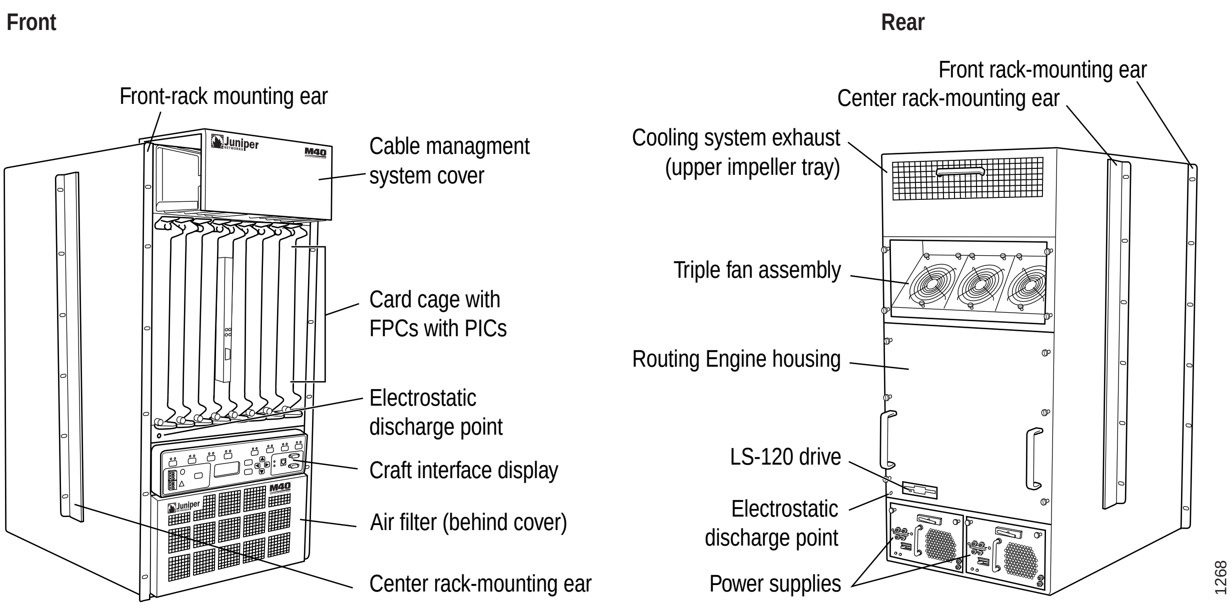
Chapter 5

M40 Internet Router Overview

NOTE: See the End-of-sale and End-of-service Announcement for the M40 routing platform and products at https://www.juniper.net/support/eol/.

The M40 Internet router provides high-speed forwarding performance, packet processing, and port density for high-growth core IP networks. The M40 router supports the JUNOS software which provides router configuration and monitoring. (See Figure 5.)

Figure 5: M40 Router



The M40 router includes the router-specific System Control Board (SCB). The SCB contains the Internet Processor II application-specific integrated circuit (ASIC) and performs sampling, filtering, and packet forwarding decisions. The SCB processes exception and control packets, monitors system components, and controls Flexible PIC Concentrator (FPC) resets.

Physical Interface Cards (PICs) are available in supported media types, including Asynchronous Transfer Mode (ATM), Channelized, DS3, E1, E3, T1, Ethernet, SONET/SDH, and IP services. The M40 router provides the bandwidth to grow networks to OC48c/STM16 speeds. The M20 and M40 FPCs and PICs are interchangeable, and most of the PICs can also be used in the M40e Internet router. For more information about supported PICs and FPCs for each M-series router type, see the appropriate PIC installation guide.

The M40 router Internet processor II ASIC forwards packets at a throughput rate of up to 40 Gigabits per second (Gbps). The ASIC technology provides such packet processing as route lookups, filtering, sampling, rate limiting, load balancing, buffer management, switching, and encapsulation and de-encapsulation of IP services. The M40 router delivers the bandwidth required to grow networks to OC48c/STM16 speeds in a cost-effective manner.

M40 Router Components

Table 7 lists the major M40 router components and characteristics.

Table 7: M40 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Cooling system	2 impeller trays and 1 fan assembly (3 fans)	Cools router components	Yes	Hot-removable, hot-insertable	–
Craft interface	1	Displays the status and allows you to perform control functions	–	Hot-removable, hot-insertable	–
FPC	1–8	Connects PICs to other components and houses shared memory	–	Hot-removable, hot-insertable	Yes
PIC	1–4 per FPC	Provides interfaces to various network media	–	Hot-removable, hot-insertable	–
Power supply	2 AC or 2 DC	Distributes voltages to components	Yes	Hot-removable, hot-insertable	–
Routing Engine	1	Handles routing protocols and maintains routing tables	–	Hot-pluggable	–
SCB	1	Performs router lookups, monitors systems, and transfers control packets	–	Hot-pluggable	–

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.

- Requires router shutdown—You must power down the router before removing the component.

Monitoring M40 Router Components

See the following chapters for information about monitoring the M40 router components:

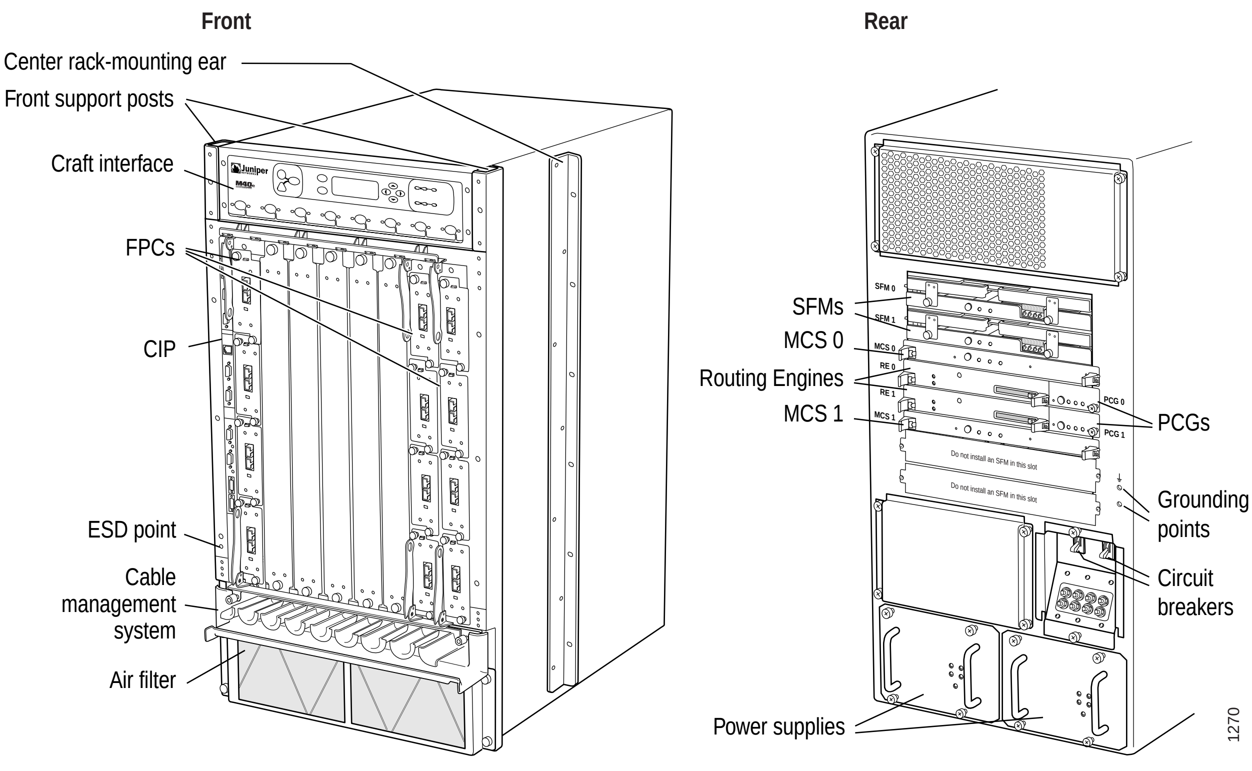
- "Monitoring the Router Chassis" on page 107
- "Monitoring the Routing Engine" on page 125
- "Monitoring Redundant Routing Engines" on page 491
- "Monitoring FPCs" on page 163
- "Monitoring PICs" on page 183
- "Monitoring the Craft Interface" on page 197
- "Monitoring Power Supplies" on page 217
- "Monitoring Redundant Power Supplies" on page 507
- "Monitoring the Cooling System" on page 251
- "Monitoring Redundant Cooling System Components" on page 523
- "Maintaining the Cable Management System, Cables, and Connectors" on page 275
- "Monitoring the SCB" on page 393

Chapter 6

M40e Internet Router Overview

The M40e Internet router provides a dense, highly redundant platform primarily for dedicated access aggregation at the edge as well as for mid-size core IP networks. The M40e router supports the JUNOS software which provides router configuration and monitoring. (See Figure 6.)

Figure 6: M40e Router



The M40e router shares the same chassis and many of the same components as the M160 Internet router. It accepts both AC and DC power supplies. The M40e router can have up to two Switching and Forwarding Modules (SFMs). The SFMs contain the Internet Processor II application-specific integrated circuit (ASIC) and two Distributed Buffer Manager ASICs, and make forwarding decisions, distribute packets throughout memory, and forward notification of outgoing packets.

The M40e router includes the host module that constructs routing tables, performs system management functions, and generates the SONET/SDH clock signal for SONET/SDH interfaces. The host module contains the Routing Engine and the Miscellaneous Control Subsystem (MCS). The Routing Engine manages routing protocols and maintains the routing tables. For a host module to function, both of these components must be installed and operational.

The M40e router houses three types of Flexible PIC Concentrators (FPCs): one to accommodate M20 and M40 Physical Interface Cards (PICs), and two to accommodate hot-swappable M160 router PICs. The Type 1 FPCs for the M40e and M160 routers are interchangeable.

PICs are available in supported media types, including Asynchronous Transfer Mode (ATM), Channelized DS3, E1, E3, T1, Ethernet, SONET/SDH, and IP services. For more information about supported PICs and FPCs for each M-series router type, see the appropriate PIC installation guide.

The M40e router Internet Processor II ASIC forwards packets at a throughput rate of up to 40 Gigabits (Gbps). The ASIC technology provides such packet processing as rate limiting, filtering, and IP services sampling.

M40e Router Major Hardware Components

Table 8 lists the major M40e router components and characteristics.

Table 8: M40e Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Connector Interface Panel (CIP)	1	Provides ports for external management and alarm relay devices	–	Requires router shutdown	–
Cooling system	3 impellers, 1 fan tray	Cools router components	Yes	Hot-removable, hot-insertable	–
Craft interface	1	Displays status information	–	Hot-removable, hot-insertable	–
FPC	1–8	Connects PICs to other components and houses shared memory	–	Hot-removable, hot-insertable	Yes
Host module	1–2	Handles routing protocols and maintains routing tables	Yes	Hot-pluggable	–
MCS	1–2	Provides system control and monitoring	Yes	Hot-pluggable	Yes
PFE Clock Generator (PCG)	2	Provides a 125-MHz system clock	Yes	Hot-pluggable	Yes
PIC	1–4 per FPC	Provides interfaces to various network media	–	Hot-removable, hot-insertable	Yes
Power supply (AC or DC)	2	Distributes power to components	Yes	Hot-removable, hot-insertable	–
Routing Engine	1–2	Manages routing protocols and maintains routing tables	Yes	Hot-pluggable	–
SFM	1–2	Provides packet switching, packet forwarding, and route lookup	Yes	Hot-pluggable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M40e Router Components

See the following chapters for information about monitoring the M40e router components:

- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring Redundant Routing Engines” on page 491
- “Monitoring FPCs” on page 163
- “Monitoring PICs” on page 183
- “Monitoring the Craft Interface” on page 197
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507
- “Monitoring the Cooling System” on page 251
- “Monitoring Redundant Cooling System Components” on page 523
- “Maintaining the Cable Management System, Cables, and Connectors” on page 275
- “Monitoring the Host Module” on page 341
- “Monitoring the SFMs” on page 347
- “Monitoring Redundant SFMs” on page 577
- “Monitoring the MCS” on page 359
- “Monitoring Redundant MCSs” on page 567
- “Monitoring the PCG” on page 369

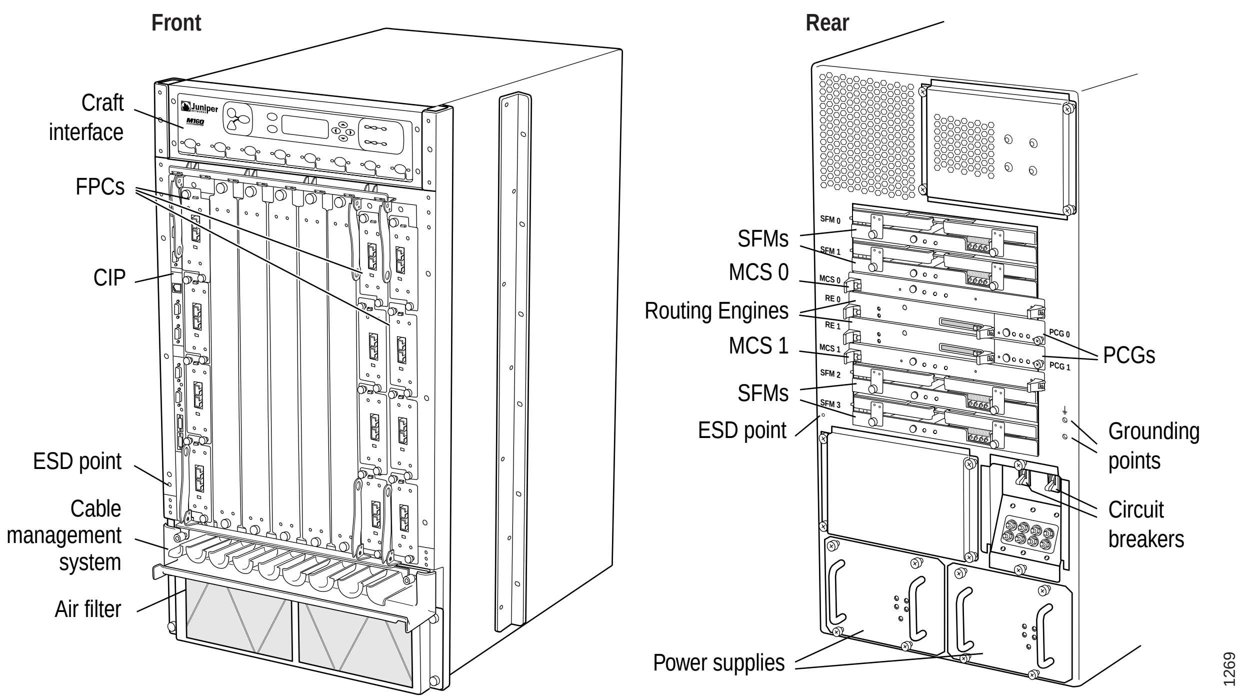
- “Monitoring Redundant PCGs” on page 595
- “Monitoring the CIP” on page 381

Chapter 7

M160 Internet Router Overview

The M160 Internet router provides a dense, highly redundant platform primarily for large backbone core IP networks where switching fabric and Routing Engine redundancy are required. The M160 router supports the JUNOS software which provides router configuration and monitoring. (See Figure 7.)

Figure 7: M160 Router



The Type 1 Flexible PIC Concentrators (FPCs) for the M40e and M160 routers are interchangeable. The M160 router supports two types of FPCs: FPC1 supports Physical Interface Cards (PICs), including the single-port OC12 and Gigabit Ethernet; and FPC2 supports higher-speed PICs, including OC48 and Tunnel Services. The router can operate with any combination of FPC1s and FPC2s installed. For more information about supported PICs and FPCs for each M-series router type, see the appropriate PIC installation guide.

The M160 router accepts only DC power supplies.

The M160 router can have up to four Switching and Forwarding Modules (SFMs). The SFMs contain the Internet Processor II application-specific integrated circuit (ASIC) and two Distributed Buffer Manager ASICs, and make forwarding decisions, distribute packets throughout memory, and forward notification of outgoing packets.

The M160 router includes the host module that constructs routing tables, performs system management functions, and generates the SONET/SDH clock signal for SONET/SDH interfaces. The host module contains the Routing Engine and the Miscellaneous Control Subsystem (MCS). The Routing Engine manages routing protocols and maintains the routing tables. For a host module to function, both of these components must be installed and operational.

PICs are available in supported media types, including Asynchronous Transfer Mode (ATM), Channelized DS3, E1, E3, T1, Ethernet, SONET/SDH, and IP services. The M160 router supports both M160 and M40e PICs. For more information about supported PICs for each M-series router type, see the appropriate PIC installation guide.

The M160 router Internet Processor II ASIC forwards packets at a throughput rate of up to 160 Gbps. The ASIC technology provides such packet processing as route lookups, filtering, sampling, rate limiting, load balancing, buffer management, switching, and encapsulation and de-encapsulation of IP services.

M160 Router Major Hardware Components

Table 9 lists the major M160 router components and characteristics.

Table 9: M160 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-replaceable	Offline Button
CIP	1	Provides ports for external management, BITS interfaces, and alarm relay devices	–	Requires router shutdown	–
Cooling system	3 impellers and 1 fan tray (4 fans)	Cools router components	Yes	Hot-removable	–
Craft interface	1	Displays status and allows you to perform control functions	–	Hot-removable, hot-insertable	–
FPC	1–8	Connects PICs to other components and houses shared memory	–	Hot-removable, hot-insertable	Yes
Host module	1–2	Handles routing protocols and maintains routing tables	Yes	Hot-pluggable	–
MCS	1–2	Provides system control and monitoring	Yes	Hot-pluggable	Yes
PCG	2	Provides a 125-MHz system clock	Yes	Hot-pluggable	Yes
PICs	1–4 per FPC	Provides interfaces to various network media	–	Hot-removable, hot-insertable	Yes
Power supply (DC only)	2	Distributes needed voltages to components	Yes	Hot-removable, hot-insertable	–

Component	Quantity	Function	Redundant	Field-replaceable	Offline Button
Routing Engine	1–2	Manages routing protocols and maintains routing tables	Yes	Hot-pluggable	–
SFM	1–4	Provides packet switching, packet forwarding, and route lookup	Yes	Hot-removable, hot-insertable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M160 Router Components

See the following chapters for information about monitoring and troubleshooting the M160 router components:

- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring Redundant Routing Engines” on page 491
- “Monitoring FPCs” on page 163
- “Monitoring PICs” on page 183
- “Monitoring the Craft Interface” on page 197
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507
- “Monitoring the Cooling System” on page 251
- “Monitoring Redundant Cooling System Components” on page 523
- “Maintaining the Cable Management System, Cables, and Connectors” on page 275
- “Monitoring the Host Module” on page 341
- “Monitoring the SFMs” on page 347

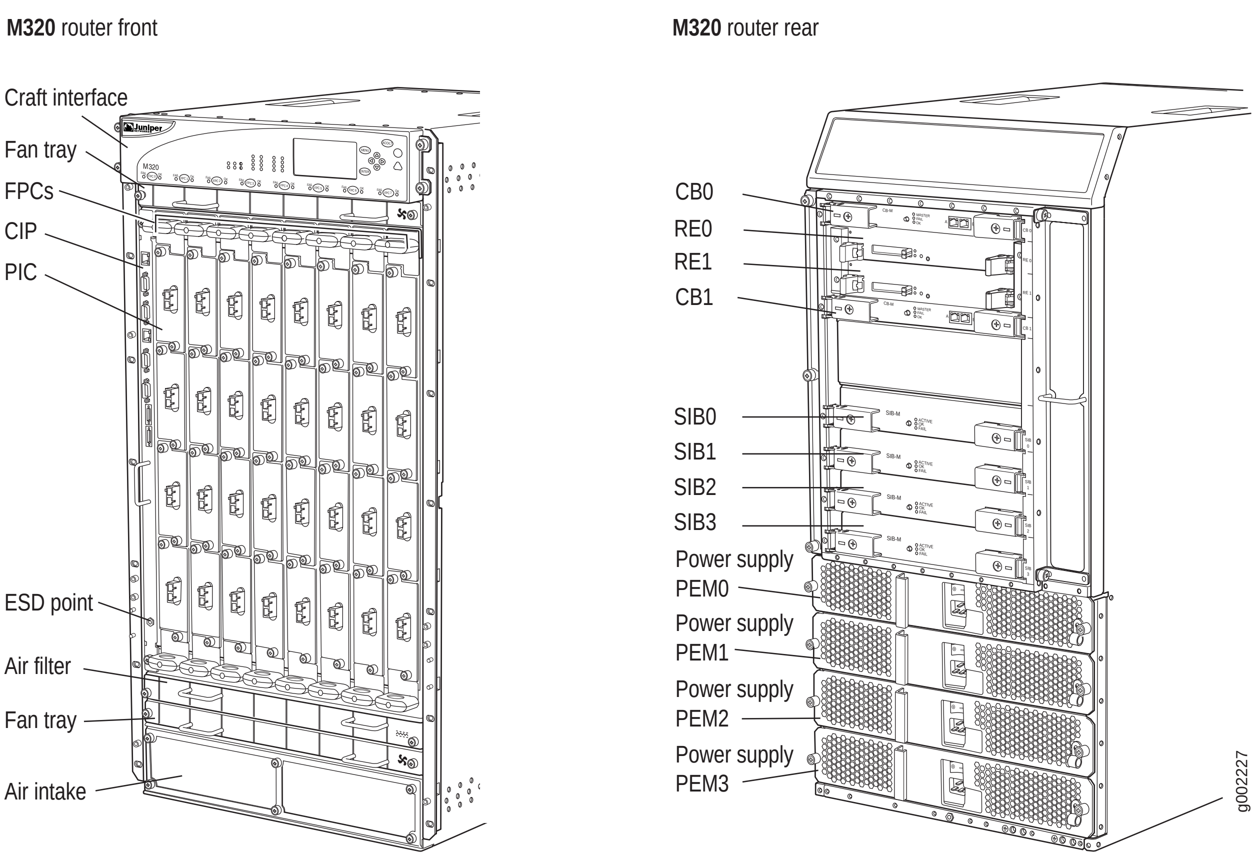
- "Monitoring Redundant SFMs" on page 577
- "Monitoring the MCS" on page 359
- "Monitoring Redundant MCSs" on page 567
- "Monitoring the PCG" on page 369
- "Monitoring Redundant PCGs" on page 595
- "Monitoring the CIP" on page 381

Chapter 8

M320 Internet Router Overview

The M320 Internet router is a high-density edge aggregation, routing, and service creation platform that can be deployed in core, peering, and data center applications. Optimized for dense edge aggregation and service creation, the M320 router can provide a single point of edge aggregation for thousands of customers over any access type, including ATM, Frame Relay, Ethernet, and Time-Division Multiplexing (TDM), at any speed from DS0 up to OC192/STM64 and 10-Gigabit Ethernet. (See Figure 8.)

Figure 8: M320 Router



The M320 router includes Switch Interface Boards (SIBs) that provide the switching function to the destination Flexible PIC Concentrator (FPC) at a total of 385 million packets per second (Mpps) of forwarding. The host subsystem, which consists of the Routing Engine and Control Board, provides the routing and system management functions of the router.

The router supports up to eight FPCs providing SONET/SDH OC-48/STM16, SONET/SDH OC192/STM64, and 160-Gigabit Ethernet media. The router supports three types of FPCs: FPC1 for hot-swappable M40e PICs, FPC2 for hot-swappable M160 PICs, and FPC3 for 10-Gbps T-series Physical Interface Cards (PICs). For more information about supported PICs, see the *M320 Internet Router PIC Guide*.

The M320 router provides a maximum aggregate throughput of 320 gigabits per second (GBps) full duplex. The JUNOS software runs on a control subsystem with dedicated hardware, ensuring that control functions are performed without affecting the forwarding subsystem. Forwarding and packet processing operations in the router are performed by dedicated programmable ASICs that enable the router to achieve data forwarding rates the match current fiber-optic capacity.

M320 Router Major Hardware Components

Table 10 lists the T320 router major components and characteristics.

Table 10: M320 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Connector Interface Panel (CIP)	1	Provides ports for external management and alarm relay devices; includes an electrostatic discharge (ESD) point	—	Hot-pluggable	—
Control Board	1–2	Monitors and controls router components (requires a Routing Engine)	Yes	Hot-pluggable (if not redundant)	Yes
Cooling system	2 front fan trays, 1 rear fan tray	Cools router components	Yes	Hot-removable, Hot insertable	—
Craft interface	1	Displays status and provides an interface for controlling router functions	—	Hot-removable. hot-insertable	—
FPC	1–8	Connects PICs to other router components, contains Packet Forwarding Engines (supports FPC1, FPC2, and FPC3)	—	Hot-removable, hot-insertable	Yes
Host subsystem	1–2	Consists of a Routing Engine and Control Board and provides routing and system management functions	Yes	Hot-pluggable	—
PIC	1–4 per FPC	Provides an interface to various network media	—	Hot-removable, hot-insertable	Yes
Power supply (DC only)	2	Distributes needed voltages to router components	Yes	Hot-removable, hot-insertable	—
Routing Engine	1–2	Provides routing functions and routing tables (requires a Control Board)	Yes	Hot-pluggable (if not redundant)	Reset button
SIB	4	Provides switching function to the destination FPC	Yes	Hot-removable, hot-insertable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring M320 Router Components

See the following chapters for information about monitoring the M320 router components:

- "Monitoring the Router Chassis" on page 107
- "Monitoring the Routing Engine" on page 125
- "Monitoring Redundant Routing Engines" on page 491
- "Monitoring the Host Subsystem" on page 289
- "Host Redundancy Overview" on page 463
- "Monitoring the Control Board" on page 301
- "Monitoring Redundant Control Boards" on page 559
- "Monitoring FPCs" on page 163
- "Monitoring PICs" on page 183
- "Monitoring the Craft Interface" on page 197
- "Monitoring Power Supplies" on page 217
- "Monitoring Redundant Power Supplies" on page 507
- "Monitoring the Cooling System" on page 251
- "Monitoring Redundant Cooling System Components" on page 523
- "Maintaining the Cable Management System, Cables, and Connectors" on page 275
- "Monitoring the SIBs" on page 325
- "Monitoring Redundant SIBs" on page 543

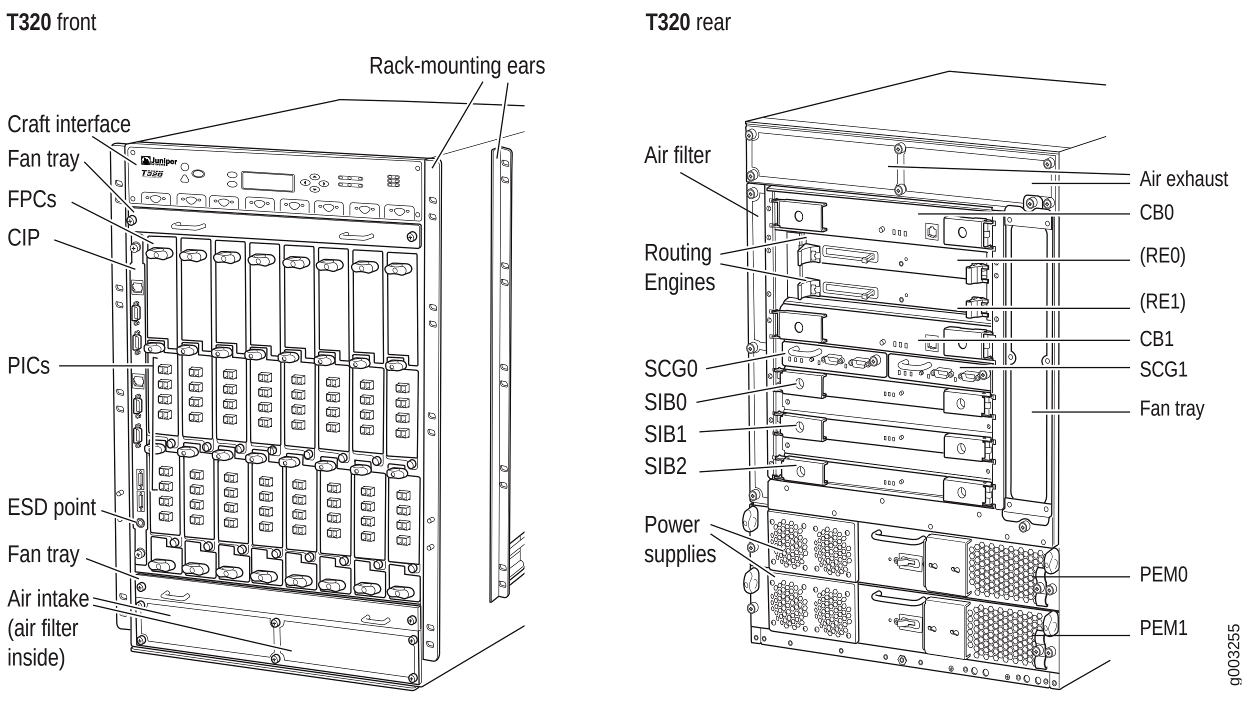
- "Monitoring the CIP" on page 381

Chapter 9

T320 Internet Router Overview

The T320 router provides 320-Gbps throughput and 385-Mpps forwarding rate and supports 16 10-Gbps (OC192c/STM64 and 10-Gigabit Ethernet) ports, as well as OC48c/STM16 for medium and large core networks, as well as for intermediate core aggregation of access routers, peering, and metro Ethernet network applications, such as those supported by Internet service providers (ISPs). It provides a cost-effective migration path to an MPLS infrastructure. The T320 router supports the JUNOS software, which provides router configuration and monitoring. (See Figure 9.)

Figure 9: T320 Router



The router supports three types of FPCs:

- FPC1—Supports PICs that are also used in the FPC1 of a Juniper Networks M-series router
- FPC2—Supports PICs that are also used in the FPC2 of a Juniper Networks M-series router and T640 Internet routing node

- FPC3—Supports higher-speed PICs that are also used in the FPC3 of a Juniper Networks T640 routing node

The router can operate with any combination of FPCs installed.

Forwarding operations in the router are performed by the Packet Forwarding Engines. Each FPC contains one Packet Forwarding Engine. The Packet Forwarding Engines receive incoming packets from the PICs installed on the FPC and forward them through the switch planes to the appropriate destination port. Each FPC contains data memory, which is managed by the Queuing and Memory Interface application-specific integrate circuits (ASICs).

PICs provide the physical connection to various network media types, receiving incoming packets from the network and transmitting outgoing packets to the network. PICs for the T320 router currently support the following network media types: ATM, ATM2, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, SONET/SDH OC3c/STM1, SONET/SDH OC12c/STM4, OC48c/STM16, OC192c/STM64, and Tunnel services. For more information on PICs used in the router, see the *T320 Internet Router PIC Guide.*

The T320 router supports two DC power supplies, which share the load evenly.

Three Switch Interface Boards (SIBs) provide the switching function to the destination FPC. The SIBs create the switch fabric for the router, providing up to a total of 320 million packets per second (Mpps) of forwarding.

Routing and system management functions of the router are performed by the host subsystem. The host subsystem consists of the Routing Engine and the Control Board.

The Routing Engine maintains the routing tables used by the router and controls the routing protocols that run on the router. Each Control Board works with an adjacent Routing Engine to provide control and monitoring functions for the router. These include determining Routing Engine mastership, controlling power, reset and SONET clocking for the other router components, monitoring and controlling fan speed, and monitoring system status using I^2C controllers.

T320 Router Major Hardware Components

Table 11 lists the T320 router major components and characteristics.

Table 11: T320 Router Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Connector Interface Panel (CIP)	1	Provides ports for external management and alarm relay devices	—	Hot-pluggable	—
Control Board	1–2	Monitors and controls router components	Yes	Hot-pluggable	Yes
Cooling system	2 front fan trays, 1 rear fan tray	Cools router components	Yes	hot-removable, hot insertable	—

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Craft interface	1	Displays status and provides an interface for controlling router functions	—	Hot-removable. hot-insertable	—
FPC	1–8	Connect PICs to other router components, contains Packet Forwarding Engines	—	Hot-removable, hot-insertable	Yes
PIC	1–2 per FPC	Provides an interface to various network media	—	Hot-removable, hot-insertable	Yes
Power supply (DC only)	2	Distributes needed voltages to router components	Yes	Hot-removable, hot-insertable	—
Routing Engine	1–2	Provides routing functions and routing tables	Yes	Hot-removable, hot-insertable	Yes
SONET Clock Generator (SCG)	1–2	Provides Stratum 3 SONET/SDH clocking	Yes	Hot-pluggable	Yes
SIB	3	Provides switch fabric	2 active, 1 standby	Hot-removable, hot-insertable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring T320 Router Components

See the following chapters for information about monitoring and troubleshooting the T320 router components:

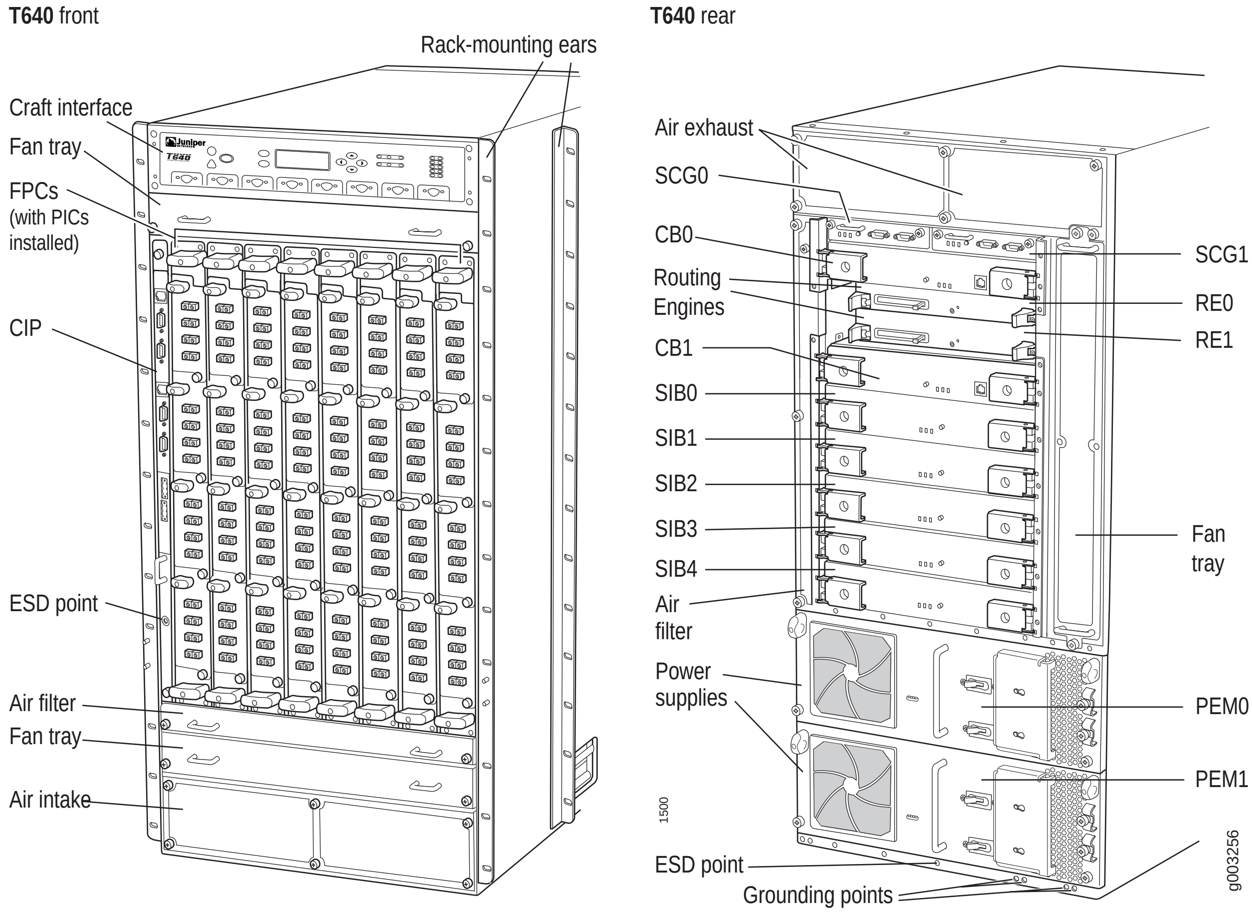
- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring Redundant Routing Engines” on page 491
- “Monitoring FPCs” on page 163
- “Monitoring PICs” on page 183
- “Monitoring the Craft Interface” on page 197
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507

Chapter 10

T640 Internet Routing Node Overview

The T640 Internet routing node provides 40G capable platform, delivering 640 Gigabits per second (Gbps) of capacity and up to 770 million packets per second (Mpps) of throughput and supports 32 10-Gbps (OC192c/STM64 and 10-Gigabit Ethernet) ports, as well as OC48c/STM16. Gigabit Ethernet, SONET/SDH, and other high-speed interfaces for large core networks and network applications, such as those supported by Internet service providers (ISPs). It provides a cost-effective migration path to an Multiprotocol Label Switching (MPLS) infrastructure. The T640 routing node supports the JUNOS software which provides router configuration and monitoring. (See Figure 10.)

Figure 10: T640 Routing Node



In a standalone configuration, the T640 routing node's maximum aggregate throughput is 320 Gbps, full duplex.

The T640 routing node supports two types of Flexible PIC Concentrators (FPCs):

- FPC2—Rated at 10 Gbps full duplex; supports PICs that are also used in the M160 router.
- FPC3—Rated at 40 Gbps full duplex; supports higher-speed PICs.

The T640 routing node can operate with any combination of FPC2s and FPC3s installed. Each FPC contains one or two Packet Forwarding Engines. The Packet Forwarding Engine consists of Layer 2/Layer 3 Packet Processing application-specific integrated circuits (ASICs), Switch Interface ASICs, T-series Internet Processor ASICs, and a memory subsystem (MMB) which includes the Queuing and Memory Interface ASICs. The Packet Forwarding Engine receives incoming packets from the PICs installed on the FPC and forwards them through the switch planes to the appropriate destination port. Each FPC contains data memory, which is managed by the Queuing and Memory Interface ASICs. Each FPC3 has two Packet Forwarding Engines, and each FPC2 has one Packet Forwarding Engine.

Physical Interface Cards (PICs) provide the physical connection to various network media types, receiving incoming packets from the network and transmitting outgoing packets to the network. PICs for the T640 routing node currently support the following network media types: Gigabit Ethernet, SONET/SDH OC12c/STM4, OC48c/STM16, OC192c/STM64, and Tunnel Services. You can install up to four PICs into the slots in each FPC. For more information on PICs used in the routing node, see the *T640 Internet Routing Node PIC Guide*.

The Switch Interface Boards (SIBs) provide the switching function to the destination FPC. The SIBs create the switch fabric for the routing node, providing up to a total of 640 million Mpps of forwarding. Five SIBs are installed in the routing node.

The host subsystem provides the routing and system management functions of the routing node. The host subsystem consists of the Routing Engine and the Control Board. The Routing Engine maintains the routing tables used by the routing node and controls the routing protocols that run on the routing node.

Each Control Board works with an adjacent Routing Engine to provide control and monitoring functions for the routing node. These include determining Routing Engine mastership; controlling power, reset, and SONET clocking for the other routing node components; monitoring and controlling fan speed; and monitoring system status using I^2C controllers.

ASICs are a definitive part of the router design; these ASICs enable the router to achieve data rates that match current fiber-optic capacity.

T640 Routing Node Major Hardware Components

Table 12 lists the major T640 routing node components and characteristics.

Table 12: T640 Routing Node Major Hardware Components

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
Connector Interface Panel (CIP)	1	Provides ports for external management and alarm relay devices	—	Hot-pluggable	—
Control Board	1–2	Monitors and controls router components	Yes	Hot-pluggable	Yes
Cooling system	2 front fan trays, 1 rear fan tray	Cools router components	Yes	hot-removable, hot insertable	—
Craft interface	1	Displays status and provides an interface for controlling router functions	—	Hot-removable. hot-insertable	—
FPC	1–8	Connect PICs to other router components, contains Packet Forwarding Engines	—	Hot-removable, hot-insertable	Yes
PIC	1–4 per FPC	Provides an interface to various network media	—	Hot-removable, hot-insertable	Yes
Power supply (DC only)	2	Distributes needed voltages to router components	Yes	Hot-removable, hot-insertable	—
Routing Engine	1–2	Provides routing functions and routing tables	Yes	Hot-removable, hot-insertable	Yes

Component	Quantity	Function	Redundant	Field-Replaceable	Offline Button
SONET Clock Generator (SCG)	1 - 2	Provides Stratum 3 SONET/SDH clockings	Yes	Hot-pluggable	Yes
SIB	5	Provides switch fabric	4 active, 1 standby	Hot-removable, hot-insertable	Yes

Field-replaceable units (FRUs) are router components that can be replaced at the customer site. Replacing FRUs requires minimal router downtime. There are three types of FRUs:

- Hot-removable and hot-insertable—You can remove and replace the component without powering down the router or interrupting the routing functions.
- Hot-pluggable—You can remove the component without powering down the router, but routing functions are interrupted until the replacement is installed.
- Requires router shutdown—You must power down the router before removing the component.

Monitoring T640 Routing Node Components

See the following chapters for information about monitoring and troubleshooting the T640 routing node components:

- “Monitoring the Router Chassis” on page 107
- “Monitoring the Routing Engine” on page 125
- “Monitoring Redundant Routing Engines” on page 491
- “Monitoring FPCs” on page 163
- “Monitoring PICs” on page 183
- “Monitoring the Craft Interface” on page 197
- “Monitoring Power Supplies” on page 217
- “Monitoring Redundant Power Supplies” on page 507
- “Monitoring the Cooling System” on page 251
- “Monitoring Redundant Cooling System Components” on page 523
- “Maintaining the Cable Management System, Cables, and Connectors” on page 275
- “Monitoring the Host Subsystem” on page 289
- “Host Redundancy Overview” on page 463

- “Monitoring the Control Board” on page 301
- “Monitoring Redundant Control Boards” on page 559
- “Monitoring the SCGs” on page 315
- “Monitoring Redundant SCGs” on page 551
- “Monitoring the SIBs” on page 325
- “Monitoring Redundant SIBs” on page 543
- “Monitoring the CIP” on page 381

Part 2

Understanding Methodology and Tools for Monitoring Router Components

Chapter 11

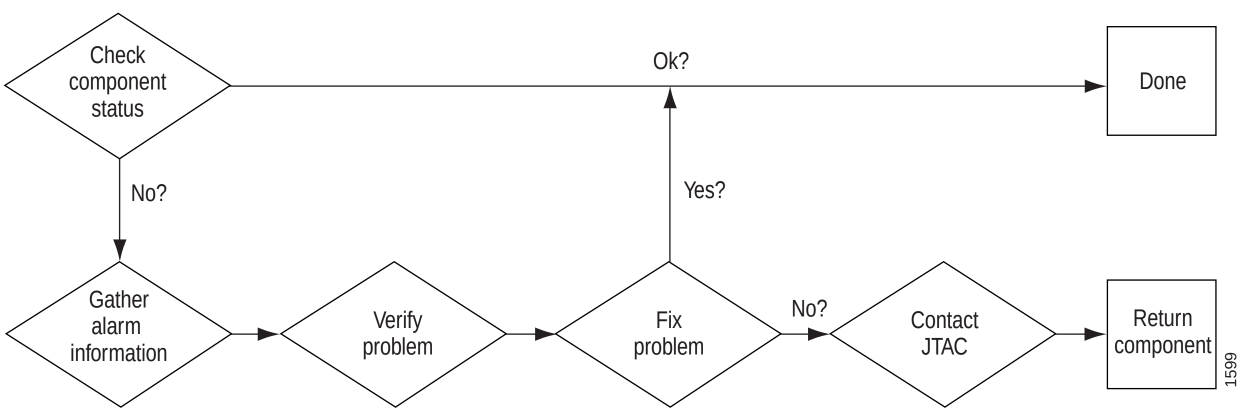
Understanding the Method and Tools for Monitoring Router Components

This chapter describes the method and tools you use to monitor and isolate problems on router hardware components. It includes the following information:

Basic Router Component Monitoring Method

Figure 11 shows the basic method you use to monitor router hardware components.

Figure 11: Basic Method for Monitoring Router Components



You should routinely monitor the status of all Juniper Networks routers running on the network.

The Simple Network Management Protocol (SNMP) network manager software running on a network management system (NMS) in the network operations center (NOC) discovers, polls, and exchanges network management information with the JUNOS software SNMP agent running on Juniper Networks routers. The SNMP network manager software collects information about router connectivity, operation, and events.

The SNMP agent responds to requests for information and controls access to its Management Information Bases (MIBs). The MIBs define all objects that can be managed on the router via SNMP. The JUNOS software chassis MIB provides environmental monitoring information on the router and its components. MIB objects represent each component and the status of the components.

A trap is generated and reported to the SNMP manager software when a significant event occurs on the router, such as an error or failure. When a trap occurs, you can log in to that router to get specific operational status information about the problem; for more information, see “Check the Router Component Status” on page 29 and “Gather Component Alarm Information” on page 33. Verify the problem and fix it if possible; for more information, see “Verify the Component Problem” on page 34 and “Fix the Problem” on page 35. If you cannot verify or fix the problem, contact the Juniper Networks Technical Assistance Center (JTAC) for more advanced analysis and troubleshooting, and return the component once failure is verified; for more information, see “Contact JTAC” on page 35 and “Return the Failed Component” on page 36.

Basic Router Component Monitoring Tools

Table 13 lists and describes the purposes of the basic tools you use to monitor router hardware.

Table 13: Basic Tools for Monitoring Router Components

Router Component Monitor Tool	Purpose
JUNOS SNMP Agent, MIBs, and traps	■ The JUNOS SNMP agent runs on Juniper Networks routers, exchanging network management information with SNMP manager software running on an NMS or host. The SNMP manager collects information about network connectivity, activity, and events by polling the router. The agent responds to requests for information and actions from the manager. ■ The SNMP agent also controls access to the agent's MIBs. The JUNOS software chassis MIB represents each component and the status of the components. ■ The agent sends a trap to the SNMP manager software when an event occurs on the router. A trap reports significant events occurring on a network device; for example, most often errors or failures.
JUNOS Software	The primary means of accessing and controlling the JUNOS software is the command-line interface (CLI). For M5, M10, M20, and M40 routers, the router provides three ports on the craft interface for connecting external management devices to the Routing Engine and hence to the JUNOS software. For M40e, M160, M320, and T320 routers, and the T640 routing node, the management ports are located on the Connector Interface Panel (CIP). For M7i and M10i routers, the management ports are located on the Routing Engine. The management ports include the following: ■ Ethernet—Used to connect the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management of the router. The Ethernet port can be 10 or 100 Mbps and uses an autosensing RJ-45 connector. The Ethernet management port has two LEDs, which indicate the type of connection in use. A yellow LED lights when a 10-Mbps connection is active, and a green LED lights when a 100-Mbps connection is active. ■ Console—Used to connect a system console to the Routing Engine with an RS-232 serial cable. ■ Auxiliary—Used to connect a laptop computer or modem to the Routing Engine with an RS-232 cable.

<table>
<tr><th>Router Component Monitor Tool</th><th>Purpose</th></tr>
<tr><td>JUNOS software CLI commands</td><td>The JUNOS software CLI has two modes: operational and configuration.

Note: You only need to type cli if you log in to the router as root. Otherwise, the CLI should be already in operational mode.

■ In operational mode, you monitor and troubleshoot the software, network connectivity, and router by entering CLI commands. To enter operational mode, log in to the router and type cli at the command prompt.

■ In configuration mode, you configure the JUNOS software that controls the router. To enter configuration mode:
a. Log in to the router.
b. Start the CLI by typing cli at the command prompt.
c. Type edit at the command prompt.

For more information about JUNOS CLI commands, see “Monitoring the CIP” on page 381.</td></tr>
</table>

Router Component Monitor Tool	Purpose
Router craft interface	The craft interface provides status and troubleshooting information at a glance and lets you perform many system control functions. The craft interface provides the following information: ■ M5 and M10 routers: Alarm LEDs and lamp test button, Routing Engine ports, link and activity status lights, and Physical Interface Card (PIC) online/offline buttons ■ M7i router: Networking interface Link/Activity LEDs, PIC On/Off LEDs, and alarm LEDs are located on the FIC ■ M10i routers: HCM status LEDs, PIC On/Off LEDs, and alarm LEDs are located on the HCM ■ M20 router: Alarm relay contacts, LEDs, and cutoff button, Routing Engine interface ports and status indicators, Routing Engine LEDs and offline buttons, Flexible PIC Concentrator (FPC) LEDs and offline button ■ M40 router: Alarm relay contacts, LEDs, cutoff button, FPC LEDs and offline button, LCD display and navigation buttons, and Routing Engine LEDs and interface ports ■ M40e router: Alarm LEDs and alarm cutoff/lamp test button, LCD display and navigation buttons, host module LEDs, and FPC LEDs and offline button ■ M160 router: Alarm LEDs and alarm cutoff/lamp test button, LCD display and navigation buttons, host module LEDs, and FPC LEDs and offline button ■ M320 router: Routing Engine LEDs, Switch Interface Board (SIB) LEDs, power supply LEDs, LCD display and navigation buttons, alarm LEDs, and FPC LEDs ■ T320 router and T640 routing node: Alarm LEDs and lamp test button, LCD display and navigation buttons, host subsystem LEDs, SIB LED, FPC LEDs, and FPC online/offline buttons The M40e, M160, and T320 routers and the T640 routing node have a CIP that contains the Alarm Relay contacts, management ports, and Link and Activity Status lights. To display craft interface information, use the following CLI command: `show chassis craft-interface`

Router Component Monitor Tool	Purpose
Router component LEDs	Router components have faceplates with LEDs that display the component status: ■ M5 and M10 routers: PICs and power supplies ■ M7i router: Compact Forwarding Engine Board (CFEB), PICs, Fixed Interface Cards (FICs) (Fast Ethernet and Gigabit Ethernet), and power supplies ■ M10i router: CFEB, High-Availability Chassis Manager (HCM), and power supplies ■ M20 router: System and Switch Boards (SSBs) and power supplies ■ M40 router: System Control Boards (SCBs) and power supplies ■ M40e router: Switching and Forwarding Modules (SFMs), Packet Forwarding Engine Clock Generators (PCGs), Miscellaneous Control Subsystem (MCS), and power supplies ■ M160 router: SFMs, PCGs, MCS, and power supplies ■ M320 router: SIBs, Control Boards, and power supplies ■ T320 router and T640 routing node: SIBs, Control Boards, SONET Clock Generators (SCGs), and power supplies To display some router component LED status, use the following CLI command: show chassis craft-interface
messages system log file	The messages system log file records the messages generated by component operational events, including error messages generated by component failures. To view the messages log file, use the following CLI command: show log messages To monitor the messages log file in real time, use the following CLI command: monitor start messages To stop monitoring the messages log file, use the following CLI command: monitor stop messages
chassisd system log file	The chassis daemon (chassisd) log file keeps track of the state of each chassis component. To view the chassisd log file, use the following CLI command: show log chassisd To monitor the chassisd log file in real time, use the following CLI command: monitor start chassisd To stop monitoring the chassisd log file, use the following CLI command: monitor stop chassisd

Router Component Monitor Tool	Purpose
Swap test	Remove the failed component. Replace it with one that you know works. Check the component status. If the replacement component works, it confirms that the original one failed.
JTAC	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States). JTAC can do more extensive testing to determine the root of the problem.

Common Operational Mode CLI Commands To Monitor Router Components

NOTE: If the Forwarding Engine Board (FEB) on M5 and M10 routers, CFEB on M10i routers, SSB on M20 routers, SCB on M40 routers, SFM on M40e and M160 routers, or SIB on M320 routers, T320 routers and the T640 routing node is not running and if you log in to the backup Routing Engine, no information about chassis components is available through the CLI.

Action To use the CLI to monitor routers, follow these steps:

1. Log in to the router.
2. At the command prompt, type **cli** to start the JUNOS software and enter operational mode.

NOTE: You only need to type **cli** if you log in to the router as root. Otherwise, the CLI should already be in operational mode.

3. Use one of the operational mode CLI commands listed in Table 14.

Table 14: Operational Mode CLI Commands for Router Monitoring

Command	Description
show version	Displays the router hostname, model number, and version of JUNOS software running on the router.
show chassis firmware	Displays firmware and operating system version for router components.
show chassis hardware	Displays an inventory of the hardware components installed in the router, including the component name, version, part number, serial number, and a brief description.
show chassis environment	Displays environmental information about the router chassis, including the temperature and status.

Command	Description
show chassis environment *component-name*	Displays more detailed operational status information about the following components: ■ M5, M10, M7i, M10i, M20 routers: Routing Engine ■ M40e and M160 routers: FPC, FPM, MCS, PCG, Power Entry Modules (PEM), Routing Engine, and SFM ■ M320 router: Control Board, FPC, FPM, PEM, Routing Engine, and SIB ■ T320 router and T640 routing node: Control Board, FPC, FPM, PEM, Routing Engine, SCG, and SIB
show chassis craft-interface	Displays operational status information about the router, including the alarm status and LED status of major components.
show chassis alarms	Displays the current router component alarms that have been generated, including the date, time, severity level, and description.
show chassis component-name	Displays more detailed operational status information about the following components: ■ M7i router: CFEB, FPC, PIC, and Routing Engine ■ M10i router: CFEB, Ethernet switch, FPC, PIC, and Routing Engine ■ M20 router: FPC, PIC, Routing Engine, and SSB ■ M40e/M160 router: Ethernet switch, FPCs, PICs, Routing Engine, and SFMs ■ M320 router: Ethernet switch, FPCs, SIBs, PICs, and Routing Engine ■ T320 router and T640 routing node: Ethernet switch, FPCs, PICs, Routing Engine, SIBs, and switch processor mezzanine board (SPMB) The command displays the total CPU DRAM and SRAM being used by the SFM processor. The command output displays the time that the SFM became active and how long the SFM has been up and running. A small uptime means that the component came online a short time ago and could indicate a possible FPC error condition.
show log messages	Displays the contents of the messages system log file that records messages generated by component operational events, including error messages generated by component failures. To monitor the messages file in real time, use the monitor start messages CLI command. This command displays the new entries in the file until you stop monitoring by using the monitor stop messages CLI command.

Command	Description
show log chassisd	Displays the contents of the chassis daemon (chassisd) log file that keeps track of the state of each chassis component To monitor the chassisd file in real time, use the monitor start chassisd CLI command. This command displays the new entries in the file until you stop monitoring by using the monitor stop chassisd CLI command.
request support information	Use this command when you contact JTAC about your component problem. This command is the equivalent of using the following CLI commands (see "Contact JTAC" on page 35): ■ show system uptime ■ show version detail ■ show system core-dumps ■ show chassis hardware ■ show system processes extensive ■ show pfe statistics error ■ show chassis routing-engine ■ show chassis environment ■ show chassis firmware ■ show chassis fpc detail ■ show system boot-messages ■ show system storage ■ show system virtual-memory ■ show system buffer ■ show system queues ■ show system statistics ■ show configuration | except SECRET-DATA ■ show interfaces extensive (for each configured interface) ■ show chassis hardware extensive

Using the Basic Monitoring Method

Steps To Take To monitor router components, follow these steps:

1. Check the Router Component Status on page 56
2. Gather Component Alarm Information on page 60
3. Verify the Component Problem on page 84
4. Fix the Problem on page 84
5. Contact JTAC on page 84
6. Return the Failed Component on page 86

Step 1: Check the Router Component Status

Steps To Take To check the router component status, follow these steps:

1. Check the Router Craft Interface on page 56
2. Check the Component LEDs on page 57
3. Display Detailed Component Environmental Information on page 59
4. Display Detailed Component Operational Information on page 60

Check the Router Craft Interface

Action To check the craft interface information for router status, do one of the following:

- Use the following CLI command:

  user@host> **show chassis craft-interface**

  The command output displays the router alarm indicator status, the LCD display information (router name, router uptime, and status message that rotates at 2-second intervals), and the major component LED status. Table 15 describes the CLI command output for each router type. For more detailed information about the craft interface, see "Monitoring the Craft Interface" on page 197.

Table 15: show chassis craft-interface CLI Command Output for Router Types

Router	CLI Command Output
M5/M10	Red alarm, Yellow alarm, Routing Engine OK, Routing Engine Fail, FPCs, and LCD screen. *Note*: Even though there is no LCD screen on the M5/M10 routers, there is still output from this command for the LCD.
M7i/M10i	Red alarm, Yellow alarm, Routing Engine OK, Routing Engine Fail, FPCs, and LCD screen. *Note*: Even though there is no LCD screen on the M7i/M10i routers, there is still output from this command for the LCD.
M20	Red alarm, Yellow alarm, Routing Engine OK, Routing Engine Fail, FPCs, and LCD screen.
M40	Red alarm, Yellow alarm, Routing Engine OK, Routing Engine Fail, FPCs, and LCD screen.
M40e/M160	FPM Display contents, Front Panel System LEDs (Routing Engine OK, Fail, Master), Front Panel Alarm Indicators (Red LED, Yellow LED, Major relay, Minor relay), Front Panel FPC LEDs, MCS LEDs, PCG LEDs, and SFM LEDs.
M320	FPM Display contents, Front Panel System LEDs (Routing Engine OK, Fail, Master), Front Panel Alarm Indicators (Red LED, Yellow LED, Major relay, Minor relay) Front Panel FPC LEDs, Control Board LEDs, SIB LEDs, and power supply (PS) LEDs.
T320/T640	FPM Display contents, Front Panel System LEDs (Routing Engine OK, Fail, Master), Front Panel Alarm Indicators (Red LED, Yellow LED, Major relay, Minor relay), Front Panel FPC LEDs, Control Board LEDs, SCG LEDs, and SIB LEDs.

- Physically look at the router craft interface. Table 16 shows the component characteristics of each router craft interface.

Table 16: Router Craft Interface Component Characteristics

Component	M5/ M10	M7i/ M10i	M20	M40	M40e	M160	M320	T320	T640
Alarm LEDs	X	X	X	X	X	X	X	X	X
Alarm cutoff/Lamp Test button (AC)/LT)	X	X	X		X	X	X	X	X
Alarm relay contacts		X	X	X	X (in CIP)	X (in CIP)		X (in CIP)	X (in CIP)
Link and activity status lights	X	X	X		X (in CIP)	X (in CIP)		X (in CIP)	X (in CIP)
LCD display and navigation buttons				X	X	X	X	X	X
Routing Engine ports	X		X	X	X (in CIP)	X (in CIP)		X (in CIP)	X (in CIP)
Routing Engine LEDs			X	X			X		
Host module LEDs					X	X			
Host subsystem LEDs								X	X
PIC online and offline buttons	X	X							
FPC LEDs	No Craft Interface	No Craft Interface	X	X	X	X	X	X	X
FPC offline buttons			X	X	X	X	X	X	X
SIB LEDs							X	X	X
Power supply LEDs							X		

Check the Component LEDs

Action To check the component LED status, do one of the following:

- Use the following CLI command:

  user@host> **show chassis craft-interface**

  The command output displays the LED status for the following components:

  - M7i/M10i/M20 router: Routing Engine and FPC
  - M40e/M160 router: Routing Engine, FPC, MCS, PCG, and SFM
  - M320 router: Routing Engine, FPC, Control Board, SIB, and power supply (PS)
  - T320 router and T640 routing node: Routing Engine, FPC, Control Board, SCG, and SIB

- Physically look at the craft interface. You see the following component LEDs:
  - M5/M10, M20, and M40 routers: Routing Engine
  - M40e/M160 routers: host module
  - T320 router and T640 routing node: host subsystem, FPCs, PICs, and SIBs
- Look at the LEDs on the component faceplate. Table 17 describes where the LEDs are located on the router.

Table 17: Component LED Location on the Router

Component	LED Location on the Router
Routing Engine	(M5/M10, M40e, and M160 routers) Remove the component cover. (M7i/M10i routers) On the Routing Engine faceplate at the front of the router. (M20 router) On the rear Routing Engine panel. (M20, M40, M40e, M160, and M320 routers) On the craft interface. ■ The M40e and M160 router Routing Engine is paired with an MCS and is monitored by the host module LEDs on the craft interface. ■ The M320 router, T320 router, and the T640 routing node Routing Engine is paired with a Control Board and is monitored by the host subsystem LEDs on the craft interface Remove the cover for the Routing Engine on the M40e, M160, and T320 routers and the T640 routing node. *Note*: You cannot see the Routing Engine LED on the M40 router.
FPC	(M20, M40, M40e, M160, and M320 routers) On the FPC faceplate at the front of the router. (M320 router) On the craft interface
PIC	(M5 and M10 routers) On the craft interface. (M7i router) On the PIC faceplate at the front of the router. (M10i router) On the FIC faceplate at the front of the router and on the PIC faceplate at front of the router. (All other routers) On the PIC faceplate at the front of the router.
Power supply	On the power supply faceplate at the bottom rear of the router. (M320 router) On the craft interface.
Host module	(M40e and M160 routers) On the craft interface. Remove the component cover.
SFM	(M40e and M160 routers) On the SFM faceplate at the rear of the router. Remove the component cover.
MCS	(M40e and M160 routers) On the MCS faceplate at the rear of the router. Remove the component cover.
PCG	(M40e and M160 routers) On the PCG faceplate at the rear of the router. Remove the component cover.
SCB	(M40 router) On the SCB faceplate at the front of the router, vertical in the middle of the FPC card cage.
SSB	(M20 router) On the SSB faceplate at the top front of the router.
Control Board	(T320 router and T640 routing node) On the Control Board faceplate at the upper rear of the chassis.

Component	LED Location on the Router
SCG	(T320 router and T640 routing node) On the SCG faceplate at the upper rear of the chassis.
SIB	(M320, T320 router and T640 routing node) On the SIB faceplate at the center rear of the chassis. (M320 router) On the craft interface.
CFEB	(M7i/M10i routers) On the DFEB faceplate at the rear of the router.
FIC	(M7i router) On the FIC faceplate at front of the router.
HCM	(M10i router) On the HCM faceplate at front of the router.

Display Detailed Component Environmental Information

(For M7i, M10i, M40e, M160, M320, and T320 routers and T640 routing node) You can display detailed environmental status information about certain router components.

Action To display detailed environmental status information about a component, use the following CLI command:

user@host> **show chassis environment** *component-name*

The command output displays the temperature of the air passing by the component, in degrees Centigrade and Fahrenheit. It also displays whether the fans and/or blowers are at normal or high speed.

Table 18 lists the operational mode CLI commands for each router component for which you can display more detailed information.

Table 18: Component Detailed Environmental Status CLI Commands

Component	Operational Mode CLI Command
FEB	show chassis environment feb
FPC	show chassis environment fpc
FPM or craft interface	show chassis environment fpm
MCS	show chassis environment mcs
PCG	show chassis environment pcg
PEM or power supply	show chassis environment pem
Routing Engine	show chassis environment routing-engine
SFM	show chassis environment sfm
Control Board	show chassis environment cb
SIB	show chassis environment sib
SCG	show chassis environment scg

Display Detailed Component Operational Information

You can display detailed operational information about certain router components. This feature is available on all routing platforms except the M5/M10, M20, and M40 routing platforms.

Action To display detailed operational information about a component, use the following CLI command:

user@host> **show chassis** *component-name*

The command output displays the temperature of the air passing by the component, in degrees Centigrade and Fahrenheit. It displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the component processor, including the total DRAM available to the component processor. The command output displays the time when the component started running and how long the component has been running. A short uptime can indicate a problem with the component.

Table 19 lists the components for which you can display more detailed operational status information.

Table 19: Component Detailed Operational Status CLI Commands

Component	Operational Mode CLI Command
CFEB	show chassis cfeb
Ethernet switch	show chassis ethernet-switch
FPC	show chassis fpc
Routing Engine	show chassis routing-engine
FEB	show chassis feb
SCB	show chassis scb
SFM	show chassis sfm
SSB	show chassis ssb
SPMB	show chassis spmb
SIB	show chassis spmb sibs
Control Board (Ethernet switch)	show chassis ethernet-switch

Step 2: Gather Component Alarm Information

Steps To Take To gather component alarm information, follow these steps:

1. Display the Current Router Alarms on page 33
2. Display Error Messages in the Messages Log File on page 33
3. Display Error Messages in the Chassis Daemon Log File on page 34

Display the Current Router Alarms

Action To display the current router component alarms, use the following CLI command:

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

The command output displays the number of alarms currently active, the time when the alarm began, the severity level, and an alarm description. Note the date and time of an alarm so that you can correlate it with error messages in the messages system log file.

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. Table 20 through Table 27 list the alarms that the chassis components can generate.

Table 20 lists the alarms that the chassis components can generate on an M5 or M10 router.

Table 20: M5 or M10 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Alternative media	The router boots from alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below required speed.	Replace the failed fan tray.	Red
FEB	The Control Board failed. If this occurs, the board attempts to reboot.	Replace the failed FEB.	Red
FPC	An FPC failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	--	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Error in reading or writing compact flash.	Reformat the compact flash and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk.	Install a bootable image on the compact flash. If this fails, replace failed Routing Engine.	Yellow
	Compact flash is missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in boot list.	Replace the failed Routing Engine.	Red
Power supplies	A power supply was removed from the chassis.	Install the missing power supply.	Yellow
	A power supply failed.	Replace the failed power supply.	Red
Temperature	The chassis temperature exceeded 55 degrees, the fans were turned on to full speed, and one or more fans failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 22 lists the alarms that the chassis components can generate on M7i and M10i routing platforms.

Table 21: M7i or M10i Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Alternative media	The router has a optional flash disk and boots from an alternate boot device. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
CFEB	For an M7i router, the CFEB failed. If this occurs, the board attempts to reboot.	Replace the failed CFEB.	Red
	For an M10i router, both Control Boards were removed or have failed.	Replace the failed or missing CFEB.	Red
	Too many hard errors in CFEB memory.	Replace the failed CFEB.	Red
	Too many soft errors in CFEB memory.	Replace the failed CFEB.	Red
	A CFEB microcode download failed.	Replace the failed CFEB.	Red
Fan trays	A fan has failed.	Replace the failed fan tray.	Red
	For an M7i router, a fan tray was removed from the chassis.	Install the missing fan tray.	Red
	For an M10i router, both fan trays are absent from the chassis.	Install the missing fan tray.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's midplane from the front is broken.	---	Red
Power supplies	A power supply was removed.	Insert missing power supply.	Yellow
	A power supply failed.	Replace the failed power supply.	Red
	For an M10i router, only one power supply is operating.	Insert or replace the secondary power supply.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk. This alarm only applies, if you have an optional flash drive.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash is missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
Temperature	The chassis temperature exceeded 55 degrees C, the fans turned on to full speed, and one or more fans failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 22 lists the alarms that the chassis components can generate on an M20 router.

Table 22: M20 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Alternative media	The router boots from alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below required speed.	Replace the fan tray.	Red
FPC	An FPC failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	---	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from the default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on the default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from the hard disk.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash is missing in the boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in the boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
Power supplies	A power supply was removed from the chassis.	Insert power supply into empty slot.	Yellow
	A power supply failed.	Replace the failed power supply.	Red
SSB	The Control Board failed. If this occurs, the board attempts to reboot.	Replace the failed Control Board.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature exceeded 55 degrees, the fans turned on to full speed, and one or more fans have failed	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 23 lists the alarms that the chassis components can generate on an M40 router.

Table 23: M40 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filter	Change the air filter.	Change the air filter.	--------------------
Alternative media	The router boots from an alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below the required speed.	Replace the fan tray.	Red
FPC	An FPC has an out-of-range or invalid temperature reading.	Replace the failed FPC.	Yellow
	An FPC microcode download has failed.	Replace the failed FPC.	Red
	An FPC failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
	Too many hard errors in FPC memory.	Replace the failed FPC.	Red
	Too many soft errors in FPC memory.	Replace the failed FPC.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	--	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Power supplies	A power supply was removed from the chassis.	Insert a power supply into an empty slot.	Yellow
	A power supply temperature sensor failed.	Replace the failed power supply or power entry module.	Yellow
	A power supply fan failed.	Replace the failed power supply fan.	Yellow
	A power supply has high temperature.	Replace the failed power supply or power entry module.	Red
	A 5V power supply has failed.	Replace the failed power supply or power entry module.	Red
	A 3.3V power supply failed.	Replace the failed power supply or power entry module.	Red
	A 2.5V power supply failed.	Replace the failed power supply or power entry module.	Red
	A power supply input failed.	Check the power supply input connection.	Red
	A power supply has failed.	Replace the failed power supply or power entry module.	Red
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on the default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
SCB	The SCB failed. If this occurs, the board attempts to reboot.	Replace the failed SCB.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature exceeded 55 degrees C, the fans turned on to full speed, and one or more fans failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees, and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 24 lists the alarms that the chassis components can generate on an M40e or M160 router.

Table 24: M40e or M160 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filter	Change the air filter.	Change the air filter.	-------------------------
Alternative media	The router boots from an alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
CIP	A CIP is missing.	Insert a CIP into an empty slot.	Red
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below the required speed.	Replace the fan tray.	Red
FPC	An FPC has an out-of-range or invalid temperature reading.	Replace the failed FPC.	Yellow
	An FPC microcode download failed.	Replace the failed FPC.	Red
	An FPC failed. If this occurs, the FPC attempts to reboot. If the MCS sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
	Too many hard errors in FPC memory.	Replace the failed FPC.	Red
	Too many soft errors in FPC memory.	Replace the failed FPC.	Red
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	----------------------------------	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
MCS	An MCS has an out-of-range or invalid temperature reading.	Replace the failed MCS.	Yellow
	An MCS was removed.	Reinstall MCS0.	Yellow
	An MCS has failed.	Replace the failed MCS.	Red
PCG	A backup PCG is offline.	Set the backup PCG online.	Yellow
	A PCG has an out-of-range or invalid temperature reading.	Replace the failed PCG.	Yellow
	A PCG was removed.	Insert a PCG into empty slot.	Yellow
	A PCG failed to come online.	Replace the failed PCG.	Red
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from the default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on the default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash is missing in the boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in the boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
Power supplies	A power supply was removed from the chassis.	Insert a power supply into the empty slot.	Yellow
	A power supply failed.	Replace the failed power supply.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
SFM	An SFM has an out of range or invalid temperature reading on SPP.	Replace the failed SFM.	Yellow
	An SFM has an out of range or invalid temperature reading on SPR.	Replace the failed SFM.	Yellow
	An SFM is offline.	Set the SFM online.	Yellow
	An SFM has failed.	Replace the failed SFM.	Red
	An SFM has been removed from the chassis.	Insert the SFM into an empty slot.	Red
	All SFMs are offline or missing from the chassis.	Insert SFMs into an empty slots or set all SFMs online.	Red
Temperature	The chassis temperature exceeded 55 degrees, the fans turned on to full speed, and one or more fans failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 25 lists the alarms that the chassis components can generate on an M320 router.

Table 25: M320 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filters	Change the air filter.	Change the air filter.	------------------------
Alternative media	The router boots from an alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Control Board	A Control Board was removed.	Insert a Control Board into the empty slot.	Yellow
	A Control Board temperature sensor alarm failed.	Replace the failed Control Board.	Yellow
	A Control Board failed.	Replace the failed Control Board.	Red
CIP	A CIP is missing.	Insert a CIP into an empty slot.	Red
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below the required speed.	Replace the fan tray.	Red
FPC	An FPC has an out of range or invalid temperature reading.	Replace the failed FPC.	Yellow
	An FPC microcode download has failed.	Replace the failed FPC.	Red
	An FPC failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
	Too many hard errors in FPC memory.	Replace the failed FPC.	Red
	Too many soft errors in FPC memory.	Replace the failed FPC.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	--	Red
Power supplies	A power supply was removed from the chassis.	Insert a power supply into the empty slot.	Yellow
	A power supply failed.	Replace the failed power supply.	Red
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from the default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk.	Install a bootable image on compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash is missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
SIB	A spare SIB is missing.	Insert a spare SIB into an empty slot.	Yellow
	An SIB failed.	Replace the failed SIB.	Yellow
	A spare SIB failed.	Replace the failed SIB.	Yellow
	An SIB has an out of range or invalid temperature reading.	Replace the failed SIB.	Yellow
	An SIB is missing.	Insert a SIB into an empty slot.	Red
	An SIB has failed.	Replace the failed SIB.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature has exceeded 55 degrees C, the fans have been turned on to full speed, and one or more fans have failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature has exceeded 65 degrees C and the fans have been turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan has failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	Chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor has failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 26 lists the alarms that the chassis components can generate on an T320 router.

Table 26: T320 Router Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filters	Change the air filter.	Change the air filters.	------------------------
Alternative media	The router boots from alternate boot device: the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net /support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Control Board	A Control Board was removed.	Insert a Control Board into an empty slot.	Yellow
	A Control Board temperature sensor alarm failed.	Replace the failed Control Board.	Yellow
	A Control Board failed.	Replace the failed Control Board.	Red
CIP	A CIP is missing.	Insert a CIP into an empty slot.	Red
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan Trays	One fan tray has been removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays have been removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or spinning below require speed.	Replace the fan tray.	Red
FPC	An FPC has an out-of-range or invalid temperature reading.	Replace the failed FPC.	Yellow
	An FPC microcode download has failed.	Replace the failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
	Too many hard errors in FPC memory.	Replace the failed FPC.	Red
	Too many soft errors in FPC memory.	Replace the failed FPC.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	------------------------------------	Red
Power supplies	A power supply was removed from the chassis.	Insert a power supply into an empty slot.	Yellow
	A power supply failed.	Replace the failed power supply.	Red
Routing Engine	Error in reading or writing hard disk.	Reformat hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install bootable image. If this fails, replace failed Routing Engine.	Yellow
	System booted from default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from hard disk.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk missing in boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
SIB	A spare SIB is missing.	Insert the spare SIB into an empty slot.	Yellow
	An SIB has failed.	Replace the failed SIB.	Yellow
	A spare SIB has failed.	Replace the failed SIB.	Yellow
	A SIB has an out-of-range or invalid temperature reading.	Replace the failed SIB.	Yellow
	An SIB is missing.	Insert an SIB into an empty slot.	Red
	An SIB has failed.	Replace the failed SIB.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Temperature	The chassis temperature exceeded 55 degrees, the fans turned on to full speed, and one or more fans failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	Chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Table 27 lists the alarms that the chassis components can generate on a T640 routing node.

Table 27: T640 Routing Node Chassis Component Alarm Conditions

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Air filter	Change the air filter.	Change the air filter.	------------------------
Alternative media	The router boots from alternate boot device, the hard disk. Typically, the router boots from the flash drive. If you configure your router to boot from the hard disk, ignore this alarm condition.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Yellow
Control Board	A Control Board was removed.	Insert a Control Board into an empty slot.	Yellow
	A Control Board temperature sensor alarm has failed.	Replace the failed Control Board.	Yellow
	A Control Board failed.	Replace the failed Control Board.	Red
CIP	A CIP is missing.	Insert a CIP into an empty slot.	Red
Craft interface	The craft interface failed.	Replace the failed craft interface.	Red
Fan trays	One fan tray was removed from the chassis.	Install the missing fan tray.	Yellow
	Two or more fan trays were removed from the chassis.	Install the missing fan trays.	Red
	One fan in the chassis is not spinning or is spinning below the required speed.	Replace the fan tray.	Red
FPC	An FPC has an out-of-range or invalid temperature reading.	Replace the failed FPC.	Yellow
	An FPC microcode download has failed.	Replace the failed FPC.	Red
	An FPC has failed. If this occurs, the FPC attempts to reboot. If the SCB sees that an FPC is rebooting too often, it shuts down the FPC.	Replace the failed FPC.	Red
	Too many hard errors in FPC memory.	Replace the failed FPC.	Red
	Too many soft errors in FPC memory.	Replace the failed FPC.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
Hot swapping	Too many hot-swap interrupts are occurring. This message generally indicates that a hardware component that plugs into the router's backplane from the front (generally, an FPC) is broken.	-----------------------------------	Red
Routing Engine	Error in reading or writing hard disk.	Reformat the hard disk and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	Error in reading or writing compact flash.	Reformat the compact flash and install a bootable image. If this fails, replace the failed Routing Engine.	Yellow
	System booted from the default backup Routing Engine. If you manually switched mastership, ignore this alarm condition.	Install a bootable image on the default master Routing Engine. If this fails, replace the failed Routing Engine.	Yellow
	System booted from the hard disk.	Install a bootable image on the compact flash. If this fails, replace the failed Routing Engine.	Yellow
	Compact flash is missing in boot list.	Replace the failed Routing Engine.	Red
	Hard disk is missing in boot list.	Replace the failed Routing Engine.	Red
	Routing Engine failed to boot.	Replace the failed Routing Engine.	Red
Power supplies	A power supply was removed from the chassis.	Insert a power supply into an empty slot.	Yellow
	A power supply has failed.	Replace the failed power supply.	Red
SCG	A backup SCG is offline.	Set the backup SCG online.	Yellow
	An SCG has an out-of-range or invalid temperature reading.	Replace the failed SCG.	Yellow
	An SCG was removed.	Insert an SCG into an empty slot.	Yellow
	All SCGs are offline or missing.	Insert SCGs into empty slots or set all SCGs online.	Red
	An SCG failed.	Replace the failed SCG.	Red

Chassis Component	Alarm Condition	Remedy	Alarm Severity
SIB	A spare SIB is missing.	Insert a spare SIB into an empty slot.	Yellow
	An SIB failed.	Replace the failed SIB.	Yellow
	A spare SIB failed.	Replace the failed SIB.	Yellow
	A SIB has an out-of-range or invalid temperature reading.	Replace the failed SIB.	Yellow
	An SIB is missing.	Insert an SIB into empty slot.	Red
	An SIB failed.	Replace the failed SIB.	Red
SPMB	A local SPMB is offline.	Reset the Control Board. If this fails, replace the Control Board.	Red
Temperature	The chassis temperature exceeded 55 degrees, the fans turned on to full speed, and one or more fans have failed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and the fans have been turned on to full speed.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Yellow
	The chassis temperature exceeded 65 degrees C and a fan failed. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	Chassis temperature exceeded 75 degrees C. If this condition persists for more than 4 minutes, the router shuts down.	■ Check the room temperature. ■ Check the air filter and replace it. ■ Check the air flow. ■ Check the fan.	Red
	The temperature sensor failed.	For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).	Red

Display Error Messages in the Messages Log File

Action To display router component error messages in the messages system log file, use the following CLI command:

user@host> **show log messages**

The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Display the error messages in the messages system log file logged at least 5 minutes before and after the alarm event.

To search for specific information in the log file, use the | match *component-name* command; for example, use show log messages | match fpc. If there is a space in the component name, enclose the component name in quotation marks; for example, | match "power supply".

To search for multiple items in the log file, use the | match command followed by the multiple items, separated by the | (pipe), and enclosed in quotation marks; for example, | match "fpc | sfm | kernel | tnp".

To monitor the messages file in real time, use the monitor start messages CLI command. This command displays the new entries in the file until you stop monitoring by using the monitor stop messages CLI command.

For more information about system log messages, see the *JUNOS System Log Messages Reference.*

Display Error Messages in the Chassis Daemon Log File

Action To display router component errors in the chassis daemon (chassisd) system log file, use the following CLI command:

user@host> **show log chassisd**

The chassis daemon (chassisd) log file keeps track of the state of each chassis component.

To search for specific information in the log file, use the | match component-name command; for example, show log messages | match fpc. If there is a space in the component name, enclose the component name in quotation marks; for example, | match "power supply".

To search for multiple items in the log file, use the | match command followed by the multiple items, separated by the | (pipe), and enclosed in quotation marks; for example, | match "fpc | sfm | kernel | tnp".

To monitor the chassisd file in real time, use the monitor start chassisd CLI command. This command displays the new entries in the file until you stop monitoring by using the monitor stop chassisd CLI command.

Step 3: Verify the Component Problem

Test a component only if it is not associated with a previously reported router component failure case and if testing will not compromise the integrity of the router and other components.

Action To verify component failure, follow these steps:

1. Make sure that the component is well seated in its slot and connected to the router midplane.

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the component for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

2. Perform a swap test on the component that has failed or has a problem. Take the component offline if necessary, remove it, and replace it with one that you know works. If the replaced component works, there was a problem with the component you removed.

Step 4: Fix the Problem

Action If the router alarm condition is your responsibility, take action and correct it. For example, replace a dirty air filter, clean a fiber-optic cable, connect the component securely to the midplane, or reset the component. Otherwise, escalate the alarm condition and contact JTAC.

NOTE: Do not straighten component pins. If a component's pins are bent, return the component with a Return Material Authorization (RMA). Straightening the pins may cause intermittent problems in the future.

Step 5: Contact JTAC

JTAC performs more advanced troubleshooting. If you cannot determine the cause of a problem or need additional assistance, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

Action To provide JTAC with information about the system, use the following CLI command:

user@host> **request support information**

Include the command output in your support request.

Because the output of this command is generally quite long, you can redirect the output to a file by using the following CLI command:

user@host> **request support information | save** *filename*

The request support information command is a combination of the following CLI operational mode commands:

- show version detail—Display the current time and information about how long the router, router software, and routing protocols have been running.
- show version detail—Display version information for the JUNOS software packages and the software for each software process.
- show system core-dumps—This is a hidden command used specifically by JTAC for troubleshooting router problems.
- show chassis hardware—Display a list of all the components installed in the router chassis. The output includes the component name, version, part number, serial number, and a brief description.
- show system processes extensive—Display exhaustive system processes that are running on the router and have controlling terminal information. This option is equivalent to the UNIX top –bSId1 infinity command.
- show pfe statistics error—Display statistics about the Packet Forwarding Engine errors.
- show chassis routing-engine—Display information about the Routing Engine.
- show chassis environment—Display environmental information about the router chassis, including the temperature and information about the fans, power supplies, and Routing Engine.
- show chassis firmware—Display the version levels of the firmware running on the SCB, SFM, SSB, FEB, and FPCs.
- show chassis fpc detail—Display detailed status information for all FPCs or for a specified FPC.
- show system boot messages—Display initial messages generated by the system kernel upon boot. This is the contents of the /var/run/dmesg.boot file.
- show system storage—Display statistics about the amount of free disk space in the router's file systems. Values are displayed in 1024-byte (1-KB) blocks. This command is equivalent to the UNIX df –k command.
- show system virtual-memory—Display the usage of JUNOS kernel memory, listed first by size of allocation and then by type of usage.
- show system buffer—Display information about the buffer pool that the Routing Engine uses for local traffic, which is the routing and management traffic that is exchanged between the Routing Engine and the Packet Forwarding Engine within the router, as well as the routing and management traffic from IP (that is, from OSPF, BGP, SNMP, pings, and so on).
- show system statistics—Display system statistics for all protocols.

- show configuration | except SECRET-DATA—Display the configuration that currently is running on the router, which is the last committed configuration. If you have modified the configuration since you last committed it, the configuration information displayed by the show configuration command will be different from that displayed with the show command from the [edit] hierarchy level in JUNOS software CLI configuration mode.
- show interfaces extensive—Display static status information about router interfaces.
- show chassis hardware extensive—Display extensive information about hardware installed in the router chassis.

Step 6: Return the Failed Component

Action To return a failed component, follow these steps:

1. Determine the part number and serial number of the component. To list the numbers for all components installed in the chassis, use the following CLI command:

   user@host> **show chassis hardware**

   If the component does not appear in the hardware inventory listing, check the failed component for the attached serial number ID label.

NOTE: The cooling system components (fans and impellers) do not have serial numbers. Therefore, you will not see a serial number listed in the hardware inventory or a serial number ID label on the component.

2. Obtain a Return Materials Authorization (RMA) number from JTAC. Open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

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

   - Part number, description, and serial number of the component
   - Your name, organization name, telephone number, fax number, and e-mail address
   - Shipping address for the replacement component, including a contact name, phone number, and e-mail address
   - Description of the failure, including log messages

   The support representative will validate your request and issue an RMA number for the return of the component.

3. Pack the router or component for shipment, as described in the appropriate router hardware guide. Label the package with the corresponding RMA number.

Part 3

Monitoring Key and Common Router Components

Chapter 12
Monitoring Key Router Components

You monitor the key router components—the Routing Engine and the Packet Forwarding Engine—to ensure that the router is handling general routing operations and is forwarding packets properly. This chapter provides an overview of the these components and includes the following information:

For information about what components comprise the Packet Forwarding Engine on each routing platform, see Table 29 on page 93.

For information about monitoring the Routing Engine, see:

- Monitoring the Routing Engine on page 125
- Monitoring Redundant Routing Engines on page 491

Understanding Key Router Components

Purpose

Inspect the Routing Engine and the Packet Forwarding Engine to ensure that the router is handling general routing operations and is forwarding packets properly.

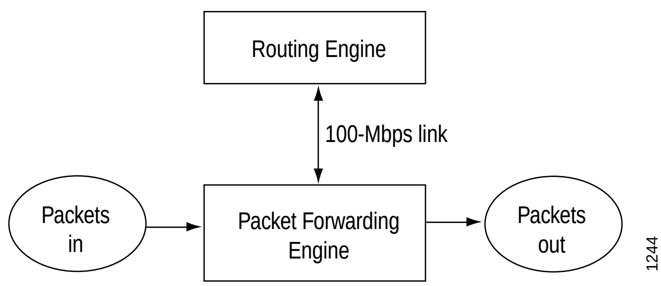
What Are the Key Router Components

The router consists of two major architectural components:

- Packet Forwarding Engine—This high-performance, application-specific integrated circuit (ASIC)-based component provides Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding.
- Routing Engine—Provides Layer 3 routing services and network management.

The Packet Forwarding Engine and the Routing Engine perform their primary tasks independently, although they constantly communicate through a 100-Mbps internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale backbone networks at high speeds. Figure 12 illustrates the relationship between the Packet Forwarding Engine and the Routing Engine.

Figure 12: Router Architecture



Packet Forwarding Engine

The Packet Forwarding Engine provides Layer 2 and Layer 3 packet switching, route lookups, packet forwarding, and route lookup functions. Table 28 lists the Packet Forwarding Engine forwarding rate and aggregate throughput for each routing platform.

Table 28: Packet Forwarding Engine Forwarding Rate and Aggregate Throughput Characteristics Per Routing Platform

Specifications	M5/ M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
Packet forwarding rate in million packets per second (Mpps)	40	16	16	40	40	40	160	385	385	770
Aggregate throughput in gigabits per second (Gbps)	6.4	8.4	12.8	25.6	40	51.2	160	320	320	640

For M-series routers, the Packet Forwarding Engine is implemented in ASICs that are located on the System Control Board (SCB): a Forwarding Engine Board (FEB) (M5/M10 router), System and Switch Board (SSB) (M20 router), SCB (M40 router), or Switching and Forwarding Module (SFM) (M40e and M160 routers). It uses a centralized route lookup engine and shared memory. For T-series routers, the Packet Forwarding Engine is implemented in ASICs that are physically located on the Flexible PIC Concentrator (FPCs) and Physical Interface Card (PICs).

Table 29 lists the Packet Forwarding Engine components for each routing platform.

Table 29: Router Packet Forwarding Engine Components Per Routing Platform

Component	M5/ M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
Midplane	X	X	X	X	X	X	X	X		
PIC	X	X	X	X	X	X	X	X	X	X
FPC	Built-in			X	X	X	X	X	X	X
FIC		X								
CFEB		X	X							
FEB	X									
SSB				X						
SCB					X					
SFM						X	X			
Layer 2/Layer 3 Packet Processing ASIC									X	X
Queuing and Memory Interface ASICs								X	X	X
T-series Internet Processor								X	X	X
Switch Interface ASICs								X	X	X
Media-specific ASICs on the PICs	X	X	X	X	X	X	X	X	X	X

Data Flow Through the Router Packet Forwarding Engine

This section describes the sequence in which data flows through each router Packet Forwarding Engine.

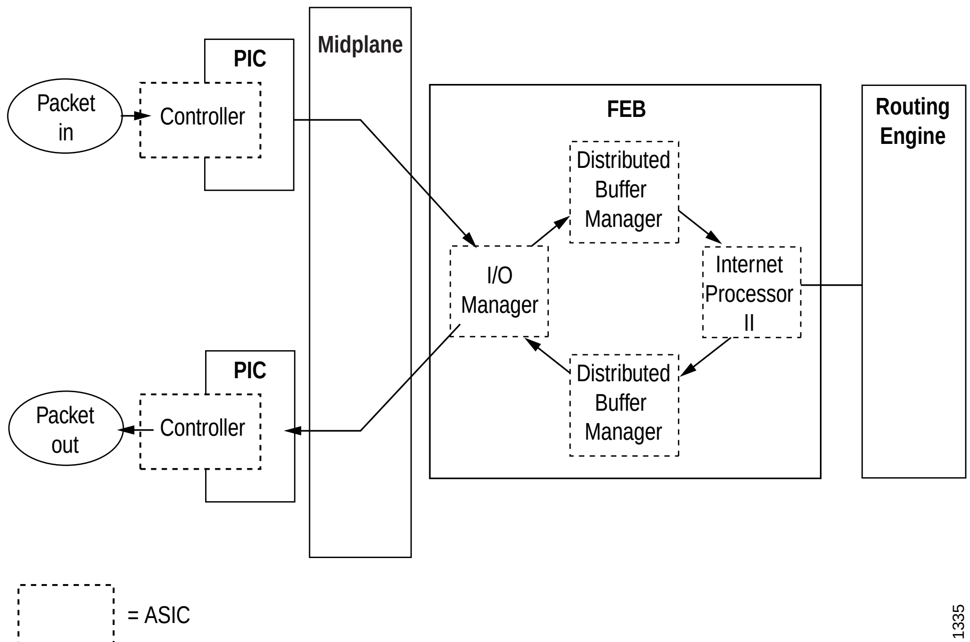
- Data Flow Through the M5 and M10 Router Packet Forwarding Engine on page 94
- Data Flow Through the M7i Router Packet Forwarding Engine on page 95
- Data Flow Through the M10i Router Packet Forwarding Engine on page 96
- Data Flow Through the M20 Router Packet Forwarding Engine on page 97
- Data Flow Through the M40 Router Packet Forwarding Engine on page 98
- Data Flow Through the M40e Router Packet Forwarding Engine on page 99
- Data Flow Through the M160 Router Packet Forwarding Engine on page 100

- Data Flow Through the M320 Router and T640 Routing Node Packet Forwarding Engine on page 101
- Data Flow Through the T320 Router and T640 Routing Node Packet Forwarding Engine on page 103

Data Flow Through the M5 and M10 Router Packet Forwarding Engine

Data flows through the M5 and M10 router Packet Forwarding Engine in the sequence shown in Figure 13:

Figure 13: M5 and M10 Router Packet Forwarding Engine Components and Data Flow

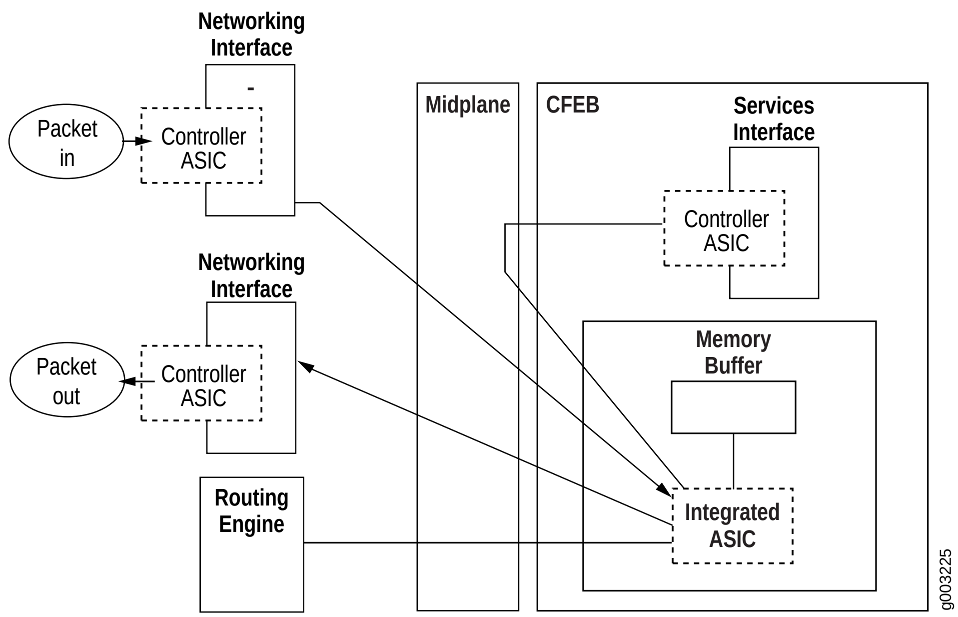


1. Packets arrive at an incoming PIC interface.
2. The PIC passes the packets through the midplane to the FEB, where the I/O Manager ASIC breaks them into 64-byte cells.
3. The Distributed Buffer Manager ASIC on the FEB distributes the data cells throughout memory banks on the FEB.
4. The Internet Processor II ASIC on the FEB performs route lookups and makes forwarding decisions.
5. The Internet Processor II ASIC notifies a second Distributed Buffer Manager ASIC on the FEB, which forwards the notification to the outgoing interface.
6. The I/O Manager ASIC on the FEB reassembles data cells in shared memory into data packets as they are ready for transmission and passes them to the outgoing PIC through the midplane.
7. The outgoing PIC transmits the data packets.

Data Flow Through the M7i Router Packet Forwarding Engine

Data flows through the M7i router Packet Forwarding Engine in the following sequence shown in Figure 14. Use of ASICs promotes efficient movement of data packets through the system.

Figure 14: M7i Router Packet Forwarding Engine Components and Data Flow



1. Packets arrive at an incoming networking interface.

2. The networking interface passes the packets to the CFEB, where the integrated ASIC processes the packet headers, divides the packets into 64-byte data cells, and distributes the data cells throughout the memory buffer.

3. The integrated ASIC on the CFEB performs a route lookup for each packet and decides how to forward it.

   a. If services are configured for the packet, the integrated ASIC reassembles the packet and passes it to the services interface.

   b. The services interface passes the packet to the CFEB, where the integrated ASIC processes the packet, divides the packet into 64-byte cells, and distributes the data cells throughout the memory buffer.

   c. The integrated ASIC performs a second route lookup for each packet and decides how to forward it.

4. The integrated ASIC notifies the outbound networking interface.

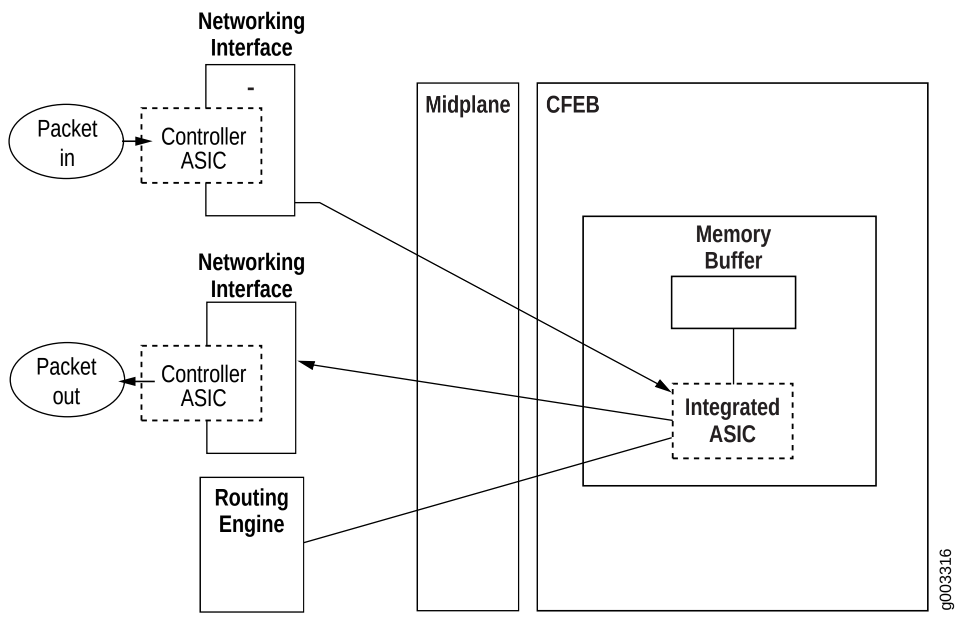
5. The integrated ASIC reassembles data cells stored in shared memory into data packets as they are ready for transmission and passes them to the outbound networking interface.

6. The outbound networking interface transmits the data packets.

Data Flow Through the M10i Router Packet Forwarding Engine

Data flows through the M10i routers Packet Forwarding Engine in the sequence shown in Figure 15. Use of ASICs promotes efficient movement of data packets through the system.

Figure 15: M10i Router Packet Forwarding Engine Components and Data Flow



1. Packets arrive at an incoming networking interface.

2. The networking interface passes the packets to the CFEB, where the integrated ASIC processes the packet headers, divides the packets into 64-byte data cells, and distributes the data cells throughout the memory buffer.

3. The integrated ASIC on the CFEB performs a route lookup for each packet and decides how to forward it.

   a. If services are configured for the packet, the integrated ASIC reassembles the packet and passes it to the services interface.

   b. The services interface passes the packet to the CFEB, where the integrated ASIC processes the packet, divides the packet into 64-byte cells, and distributes the data cells throughout the memory buffer.

   c. The integrated ASIC performs a second route lookup for each packet and decides how to forward it.

4. The integrated ASIC notifies the outbound networking interface.

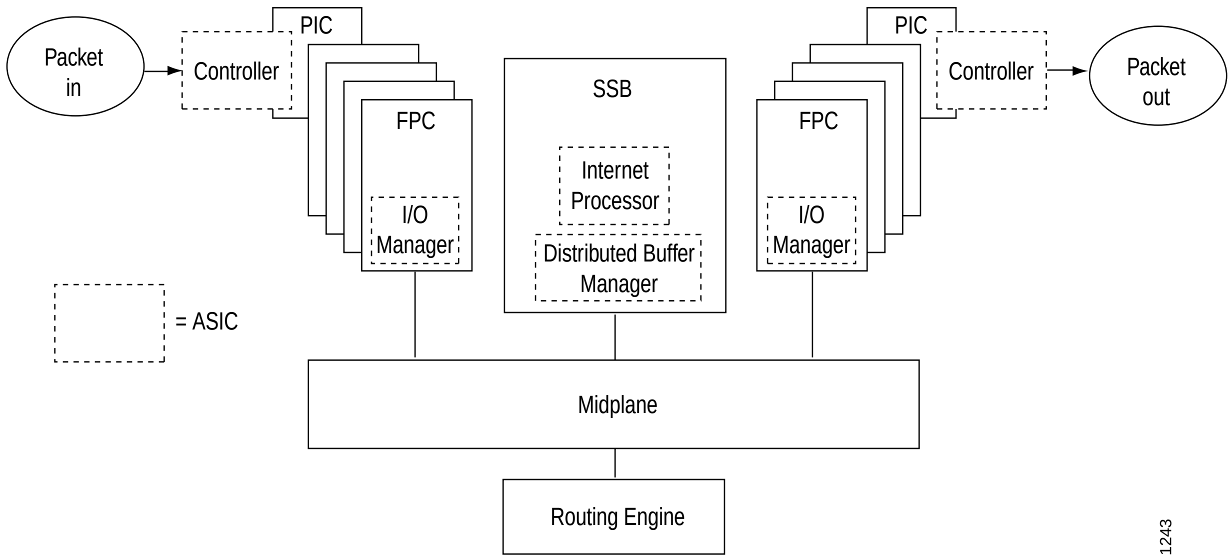
5. The integrated ASIC reassembles data cells stored in shared memory into data packets as they are ready for transmission and passes them to the outbound networking interface.

6. The outbound networking interface transmits the data packets.

Data Flow Through the M20 Router Packet Forwarding Engine

Data flows through the M20 router Packet Forwarding Engine in the sequence shown in Figure 16.

Figure 16: M20 Router Packet Forwarding Engine Components and Data Flow

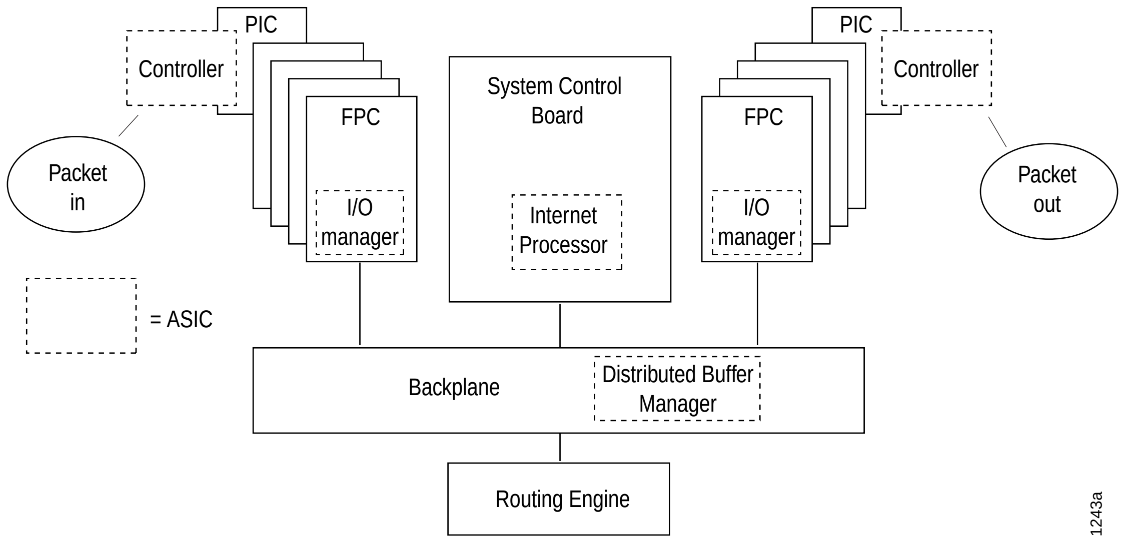


1. Packets arrive at an incoming PIC interface.
2. The I/O Manager ASIC processes the packet headers, divides the packets into 64-byte data cells, and passes the cells through the midplane to the SSB.
3. A Distributed Buffer Manager ASIC on the SSB distributes the data cells throughout the memory buffers located on and shared by all the FPCs.
4. The Internet Processor II ASIC on the SSB performs a route lookup for each packet and decides how to forward it.
5. The Internet Processor II ASIC notifies a Distributed Buffer Manager ASIC on the SSB of the forwarding decision, and the Distributed Buffer Manager ASIC forwards the notification to the FPC that hosts the appropriate outbound interface.
6. The I/O Manager ASIC on the FPC reassembles data cells stored in shared memory into data packets as they are ready for transmission and passes them through the Packet Director ASIC to the outbound PIC.
7. The outbound PIC transmits the data packets.

Data Flow Through the M40 Router Packet Forwarding Engine

Data flows through the M40 router Packet Forwarding Engine in the sequence shown in Figure 17.

Figure 17: M40 Router Packet Forwarding Engine Components and Data Flow

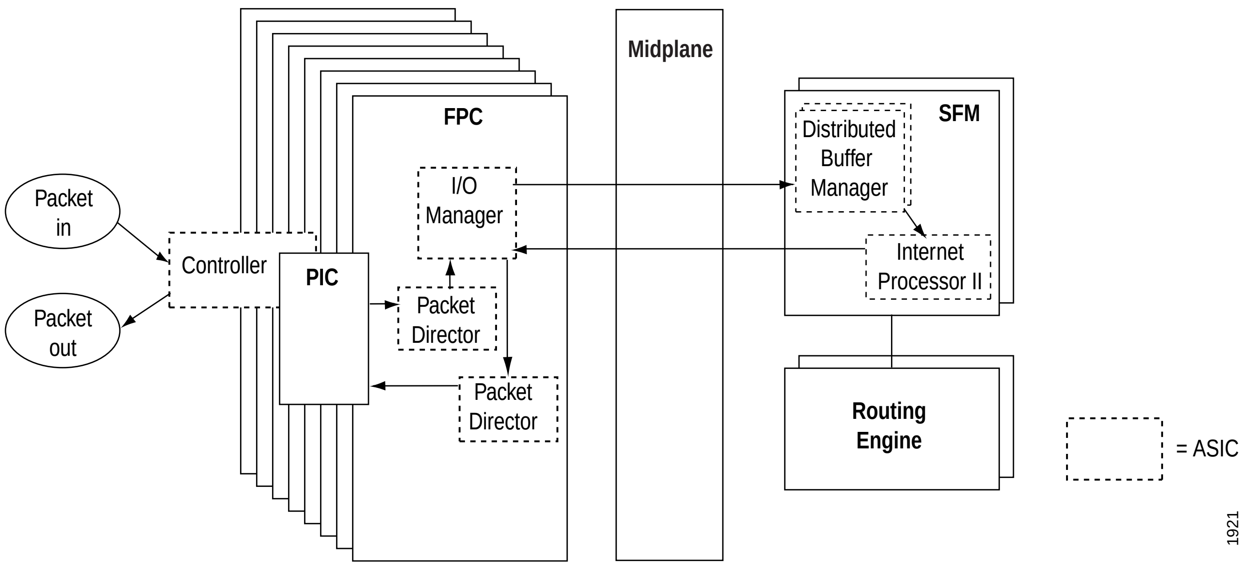


1. Packets arrive at an incoming PIC interface.
2. The PIC passes the packets to the FPC, where the I/O Manager ASIC processes the packet headers, divides the packets into 64-byte data cells, and passes the cells to the backplane.
3. The Distributed Buffer Manager ASIC on the backplane distributes the data cells throughout the memory buffers located on and shared by all the FPCs.
4. The Internet Processor or Internet Processor II ASIC on the SCB performs route lookups and makes forwarding decisions.
5. The Internet Processor or Internet Processor II ASIC notifies a second Distributed Buffer Manager ASIC on the backplane of the routing decision.
6. The Distributed Buffer Manager ASIC forwards the notification to the FPC that hosts the outbound PIC.
7. The I/O Manager ASIC on the FPC reassembles data cells in shared memory into data packets as they are ready for transmission and passes them to the outbound PIC.
8. The outbound PIC transmits the data packets.

Data Flow Through the M40e Router Packet Forwarding Engine

Data flows through the M40e router Packet Forwarding Engine in the sequence shown Figure 18.

Figure 18: M40e Router Packet Forwarding Engine Components and Data Flow



1. Packets arrive at an incoming PIC interface.

2. The PIC passes the packets to the FPC, where the Packet Director ASIC directs them to the active I/O Manager ASIC.

3. The I/O Manager ASIC processes the packet headers, divides the packets into 64-byte data cells, and passes the cells through the midplane to the SFM.

4. A Distributed Buffer Manager ASIC on the SFM distributes the data cells throughout the memory buffers located on and shared by all the FPCs.

5. The Internet Processor II ASIC on the SFM performs a route lookup for each packet and decides how to forward it.

6. The Internet Processor II ASIC notifies the second Distributed Buffer Manager ASIC (on the SFM) of the forwarding decision, and the Distributed Buffer Manager ASIC forwards the notification to the FPC that hosts the appropriate outbound interface.

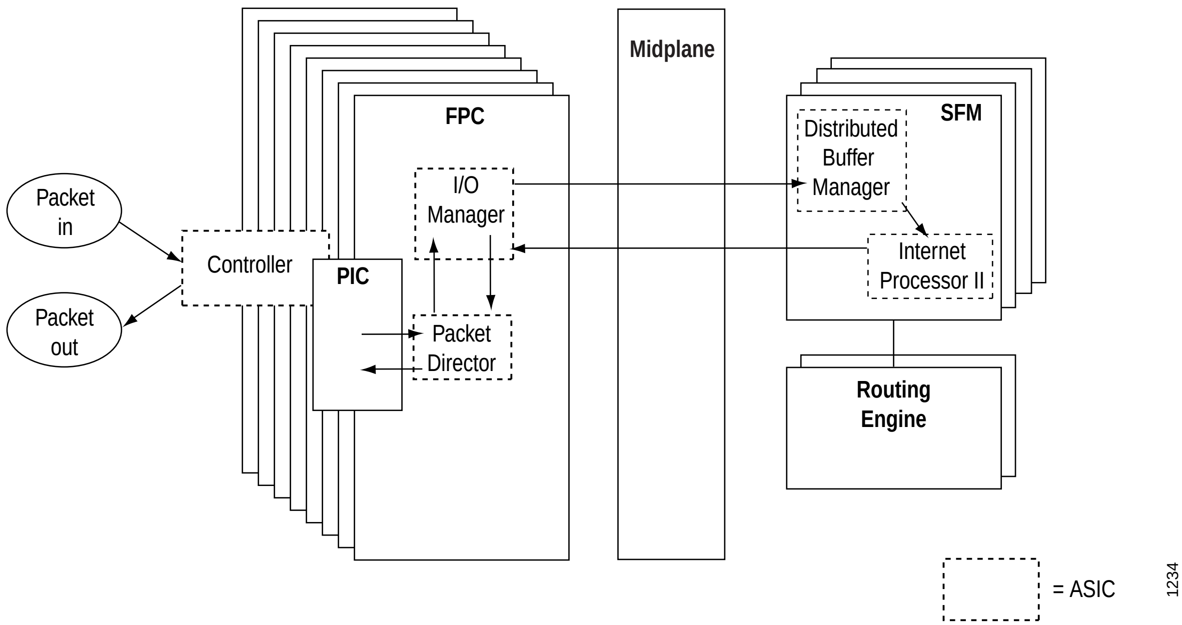
7. The I/O Manager ASIC on the FPC reassembles data cells stored in shared memory into data packets as they are ready for transmission and passes them through the Packet Director ASIC to the outbound PIC.

8. The outbound PIC transmits the data packets.

Data Flow Through the M160 Router Packet Forwarding Engine

Data flows through the M160 router Packet Forwarding Engine in the sequence shown in Figure 19.

Figure 19: M160 Router Packet Forwarding Engine Components and Data Flow

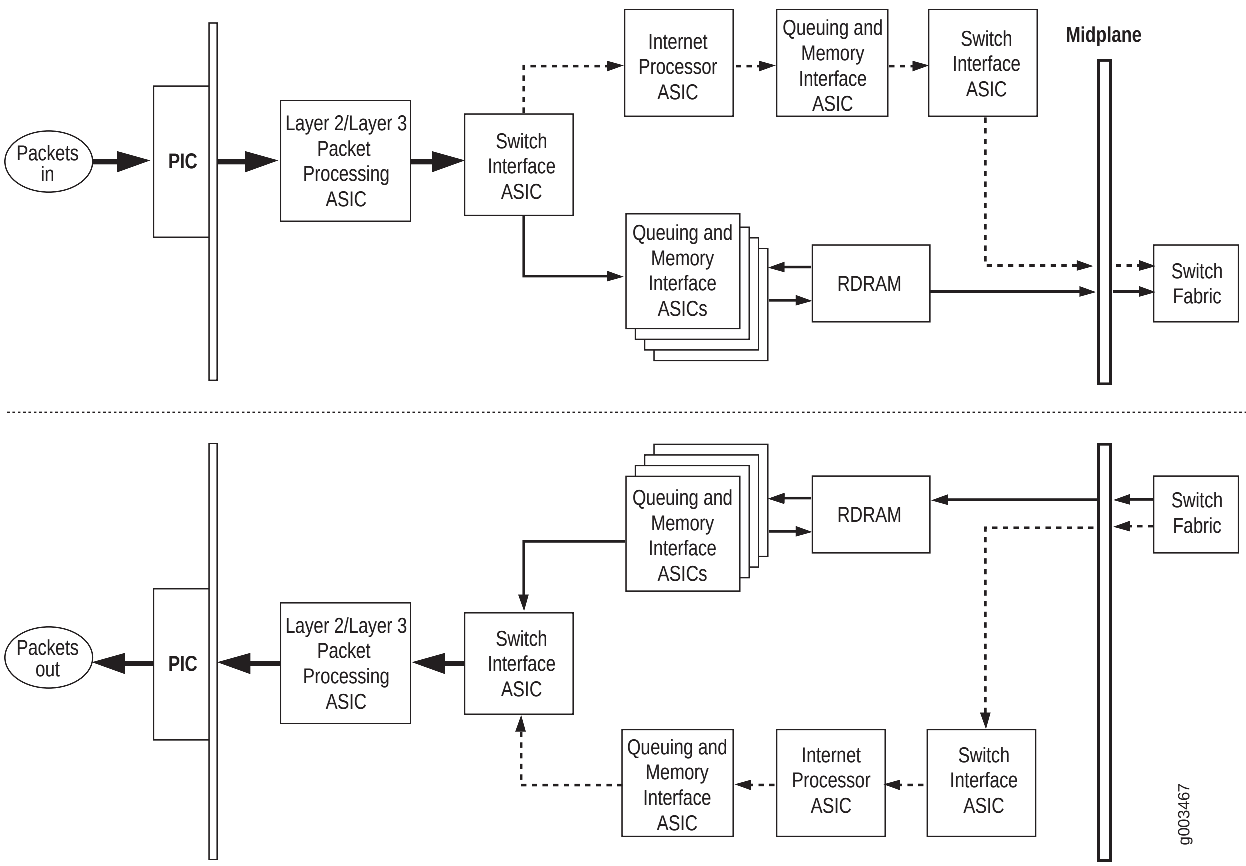


1. Packets arrive at an incoming PIC interface.
2. The PIC passes the packets to the FPC, where the Packet Director ASIC distributes them among the I/O Manager ASICs.
3. The I/O Manager ASICs process the packet headers, divide the packets into 64-byte data cells, and pass the cells through the midplane to the SFMs.
4. The Distributed Buffer Manager ASICs on the SFMs distribute the data cells throughout memory buffers located on and shared by all the FPCs.
5. For each packet, an Internet Processor II ASIC on an SFM performs a route lookup and decides how to forward the packet.
6. The Internet Processor II ASIC notifies a second Distributed Buffer Manager ASIC (on the SFM) of the forwarding decision, and the Distributed Buffer Manager ASIC forwards the notification to the FPC that hosts the appropriate outbound interface.
7. The I/O Manager ASIC on the FPC reassembles data cells in shared memory into data packets as they are ready for transmission and passes them through the Packet Director ASIC to the outbound PIC.
8. The outbound PIC transmits the data packets.

Data Flow Through the M320 Router and T640 Routing Node Packet Forwarding Engine

Data flows through the M320 routing node Packet Forwarding Engine in the sequence shown Figure 20.

Figure 20: M320 Router Packet Forwarding Engine Components and Data Flow



1. Packets arrive at an incoming PIC interface.

2. The PIC passes the packets to the FPC, where the Layer 2/Layer 3 Packet Processing ASIC performs Layer 2 and Layer 3 parsing and divides the packets into 64-byte cells.

3. The Switch Interface ASIC extracts the route lookup key, places it in a notification and passes the notification to the Internet Processor ASIC. The Switch Interface ASIC also passes the data cells to the Queuing and Memory Interface ASICs for buffering.

4. The Queuing and Memory Interface ASICs pass the data cells to memory for buffering.

5. The Internet Processor ASIC performs the route lookup and forwards the notification to the Queuing and Memory Interface ASIC.

6. The Queuing and Memory Interface ASIC sends the notification to the Switch Interface ASIC facing the switch fabric, unless the destination is on the same Packet Forwarding Engine. In this case, the notification is sent back to the Switch Interface ASIC facing the outgoing ports, and the packets are sent to the outgoing port without passing through the switch fabric (see Step 13).

7. The Switch Interface ASIC sends bandwidth requests through the switch fabric to the destination port. The Switch Interface ASIC also issues read requests to the Queuing and Memory Interface ASIC to begin reading data cells out of memory.

8. The destination Switch Interface ASIC sends bandwidth grants through the switch fabric to the originating Switch Interface ASIC.

9. Upon receipt of each bandwidth grant, the originating Switch Interface ASIC sends a cell through the switch fabric to the destination Packet Forwarding Engine.

10. The destination Switch Interface ASIC receives cells from the switch fabric. It extracts the route lookup key from each cell, places it in a notification, and forwards the notification to the Internet Processor ASIC.

11. The Internet Processor ASIC performs the route lookup, and forwards the notification to the Queuing and Memory Interface ASIC.

12. The Queuing and Memory Interface ASIC forwards the notification, including next-hop information, to the Switch Interface ASIC.

13. The Switch Interface ASIC sends read requests to the Queuing and Memory Interface ASIC to read the data cells out of memory, and passes the cells to the Layer 2/Layer 3 Packet Processing ASIC.

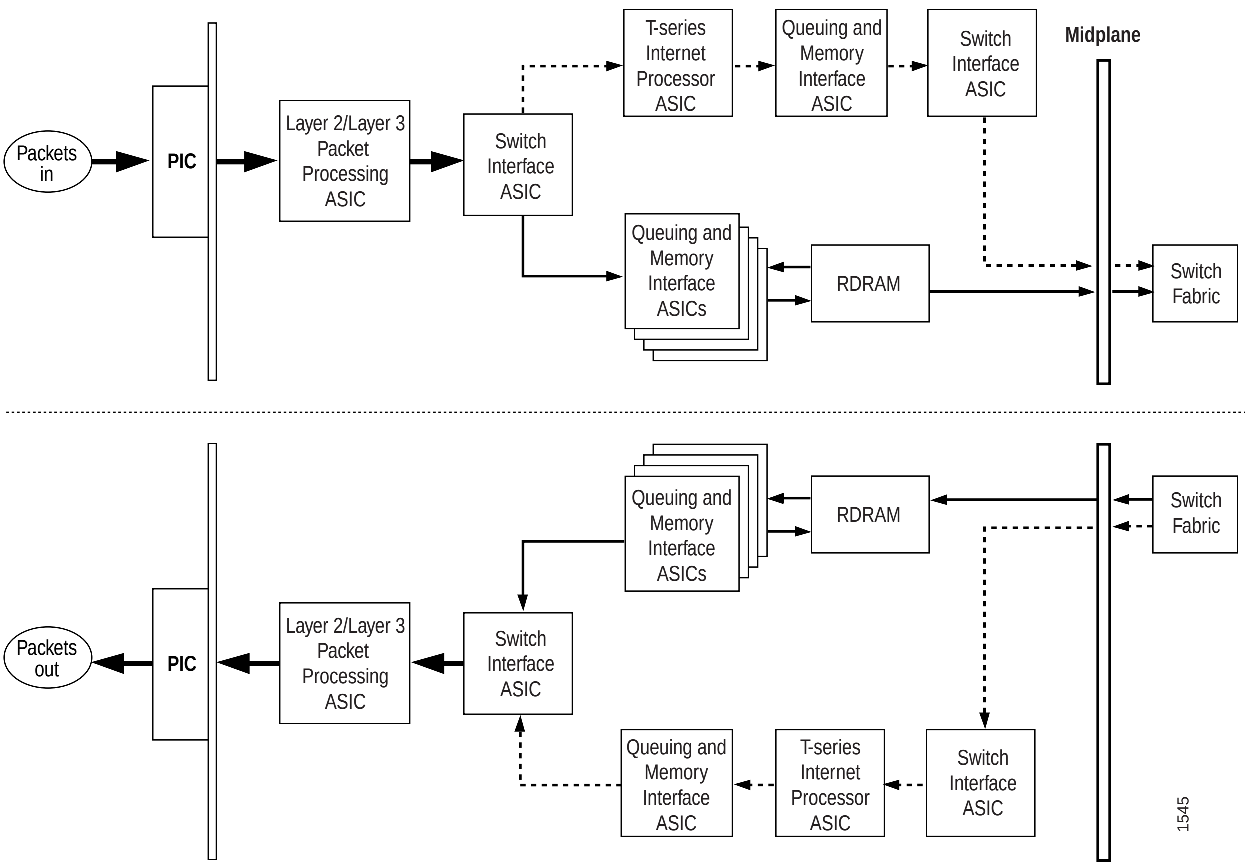
14. The Layer 2/Layer 3 Packet Processing ASIC reassembles the data cells into packets, adds Layer 2 encapsulation, and sends the packets to the outgoing PIC interface.

15. The outgoing PIC sends the packets out into the network.

Data Flow Through the T320 Router and T640 Routing Node Packet Forwarding Engine

Data flows through the T320 router and T640 routing node Packet Forwarding Engine in the following sequence shown in Figure 21.

Figure 21: T320 Router and T640 Routing Node Packet Forwarding Engine Components and Data Flow



1. Packets arrive at an incoming PIC interface.
2. The PIC passes the packets to the FPC, where the Layer 2/Layer 3 Packet Processing ASIC performs Layer 2 and Layer 3 parsing and divides the packets into 64-byte cells.
3. The Switch Interface ASIC extracts the route lookup key, places it in a notification, and passes the notification to the T-series Internet Processor. The Switch Interface ASIC also passes the data cells to the Queuing and Memory Interface ASICs for buffering.
4. The Queuing and Memory Interface ASICs pass the data cells to memory for buffering.
5. The T-series Internet Processor performs the route lookup and forwards the notification to the Queuing and Memory Interface ASIC.

6. The Queuing and Memory Interface ASIC sends the notification to the Switch Interface ASIC facing the switch fabric, unless the destination is on the same Packet Forwarding Engine. In this case, the notification is sent back to the Switch Interface ASIC facing the outgoing ports, and the packets are sent to the outgoing port without passing through the switch fabric (see Step 13).

7. The Switch Interface ASIC sends bandwidth requests through the switch fabric to the destination port. The Switch Interface ASIC also issues read requests to the Queuing and Memory Interface ASIC to begin reading data cells out of memory.

8. The destination Switch Interface ASIC sends bandwidth grants through the switch fabric to the originating Switch Interface ASIC.

9. Upon receipt of each bandwidth grant, the originating Switch Interface ASIC sends a cell through the switch fabric to the destination Packet Forwarding Engine.

10. The destination Switch Interface ASIC receives cells from the switch fabric. It extracts the route lookup key from each cell, places it in a notification, and forwards the notification to the T-series Internet Processor.

11. The T-series Internet Processor performs the route lookup, and forwards the notification to the Queuing and Memory Interface ASIC.

12. The Queuing and Memory Interface ASIC forwards the notification, including next-hop information, to the Switch Interface ASIC.

13. The Switch Interface ASIC sends read requests to the Queuing and Memory Interface ASIC to read the data cells out of memory, and passes the cells to the Layer 2/Layer 3 Packet Processing ASIC.

14. The Layer 2/Layer 3 Packet Processing ASIC reassembles the data cells into packets, adds Layer 2 encapsulation, and sends the packets to the outgoing PIC interface.

15. The outgoing PIC sends the packets out into the network.

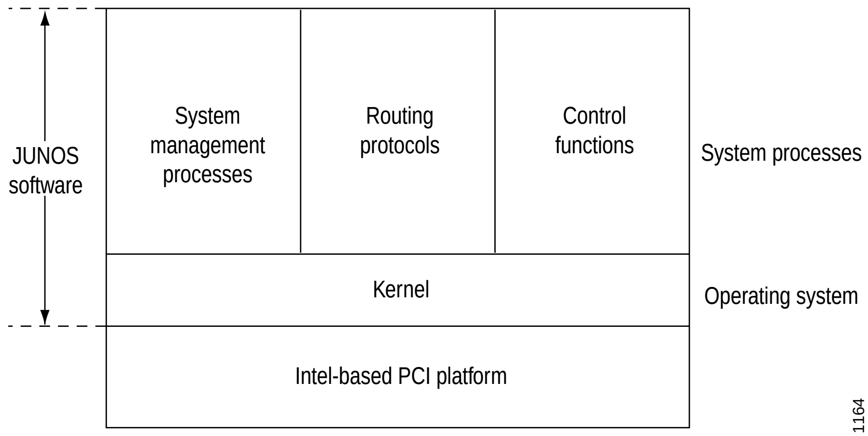
Routing Engine

The Routing Engine consists of JUNOS software running on an Intel-based Peripheral Component Interconnect (PCI) platform. The JUNOS kernel supports JUNOS system processes which handle system management processes, routing protocols, and control functions (see Figure 22 on page 105).

The Routing Engine handles all the routing protocol processes, as well as other software processes that control the router interfaces, the chassis components, system management, and user access to the router. These routing and software processes run on top of a kernel that interacts with the Packet Forwarding Engine.

The Routing Engine has a dedicated 100-Mbps internal connection to the Packet Forwarding Engine.

Figure 22: Routing Engine Architecture



Routing Engine Functions

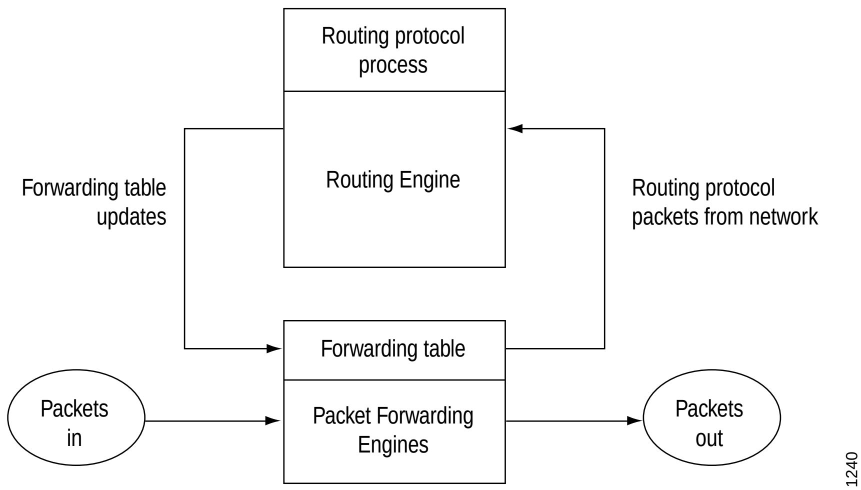
The Routing Engine handles all the routing protocol processes, as well as other software processes that control the router interfaces, system management, and user access to the router. These routing and software processes run on top of a kernel that interacts with the T-series Internet Processor in the Packet Forwarding Engine.

The Routing Engine provides the following functions:

- Routing protocol packet processing—All routing protocol packets from the network are directed to the Routing Engine, and hence do not delay the Packet Forwarding Engine unnecessarily.
- Software modularity—By dividing the different software functions into separate processes, the failure of one process is isolated from others and has little or no effect on them.
- In-depth Internet functionality—Each routing protocol is implemented with a complete set of Internet features and provides full flexibility for advertising, filtering, and modifying routes. Routing policies are set according to route parameters (such as prefix, prefix lengths, and BGP attributes).
- Scalability—The JUNOS routing tables are designed to hold all the routes in current and imminent networks. Additionally, the JUNOS software efficiently supports large numbers of interfaces and virtual circuits.
- Management interface—Different levels of system management practices are provided, including a command-line interface (CLI) and SNMP.
- Storage and change management—Configuration files, system images, and microcode can be held and maintained in primary and secondary storage systems, permitting local or remote upgrades.
- Efficiency and flexibility monitoring—The router permits alarm handling and packet counting. For example, the router allows information to be gathered on every port, without adversely affecting packet forwarding performance.

The Routing Engine constructs and maintains one or more routing tables (see Figure 23). From the routing tables, the Routing Engine derives a table of active routes, called the *forwarding table*, which is copied into the Packet Forwarding Engines. The design of the T-series Internet Processor allows the forwarding table in the Packet Forwarding Engines to be updated without interrupting the router's forwarding.

Figure 23: Control Packet Handling for Routing and Forwarding Table Update



On the M320 and T320 routers and the T640 routing node, the host subsystem provides the routing and system management functions. The host subsystem consists of the Routing Engine and the Control Board. For more information about the host subsystem, see "Monitoring the Host Subsystem" on page 289. For more information about the Control Boards, see "Monitoring the Control Board" on page 301.

On the M40e and M160 routers, the host module provides the routing and system management functions. The host module consists of the Routing Engine and the Miscellaneous Control Subsystem (MCS). For more information about the host module, see "Monitoring the Host Module" on page 341. For more information about the MCS, see "Monitoring the MCS" on page 359.

On the M10i router, the Routing Engine works with its companion High-Availability Chassis Manager (HCM) to provide control and monitoring functions for router components. For more information about the HCM, see "Monitoring the HCM" on page 431.

Chapter 13

Monitoring the Router Chassis

You monitor the router to ensure that the installed components are operating normally and that packets are being received and forwarded to their destination. (See Table 30.)

Table 30: Checklist for Monitoring the Router Chassis

Monitor Chassis Tasks	Command or Action
Understanding the Router Chassis on page 108	
■ M5 and M10 Router Chassis and Components on page 109	
■ M7i Router Chassis and Components on page 109	
■ M10i Router Chassis and Components on page 110	
■ M20 Router Chassis and Components on page 110	
■ M40 Router Chassis and Components on page 111	
■ M40e Router Chassis and Components on page 112	
■ M160 Router Chassis and Components on page 113	
■ M320 Router Chassis and Components on page 114	
■ T320 Router Chassis and Components on page 115	
■ T640 Routing Node and Components on page 116	
Checking the Router Chassis Component Status on page 117	
1. Display the Hardware Components Installed in the Router Chassis on page 117	show chassis hardware
2. Check the Component Environmental Status on page 118	show chassis environment
3. Check the Component Status from the Craft Interface on page 118	show chassis craft-interface
Checking Router Alarms on page 119	
1. Display Current Component Alarms on page 120	show chassis alarms show chassis craft-interface
2. Display Component Error Messages in the System Log File on page 121	show log messages
3. Display Component Errors in the Chassis Daemon Log File on page 122	show log chassisd

Monitor Chassis Tasks	Command or Action
Verifying Router Component Failure on page 122	Replace the failed component with one that you know works and check its status.
Replacing a Failed Component on page 122	1. Locate the component serial number ID label. 2. Obtain a Return Material Authorization (RMA) from JTAC. 3. Pack the component and ship it. See "Return the Failed Component" on page 86, or follow the procedures in the appropriate router hardware guide.

Understanding the Router Chassis

Purpose Monitor the router chassis to ensure that the installed components are operating normally and that packets are being forwarded to their destination.

What Is a Chassis The router chassis is a rigid sheet-metal structure that houses all of the router hardware components. For more information about the router chassis, see the appropriate router hardware guide.

Figure 24 shows the front and rear of the M5 and M10 Internet router chassis and the installed components.

Figure 24: M5 and M10 Router Chassis and Components

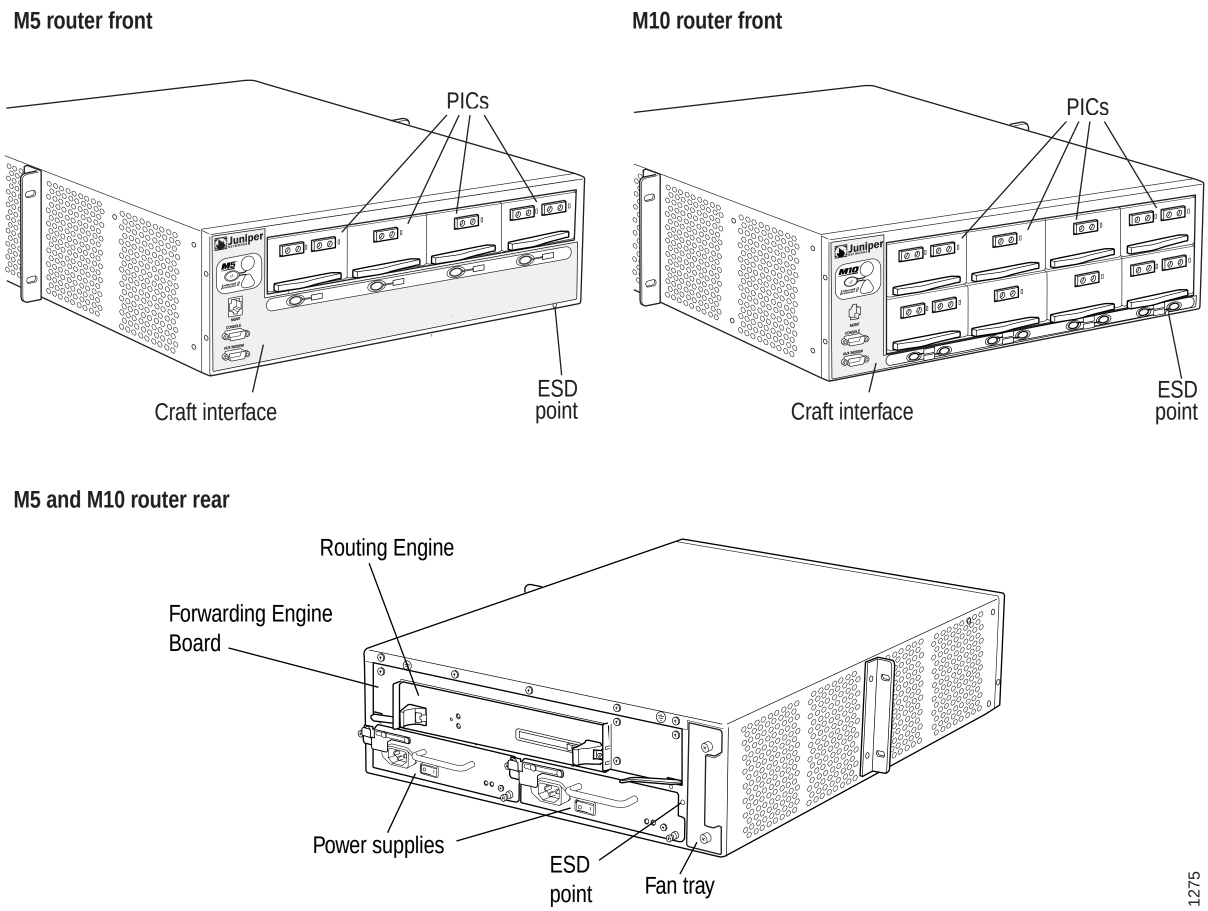


Figure 25 shows the front and rear of the M7i Internet router chassis and the installed components.

Figure 25: M7i Router Chassis and Components

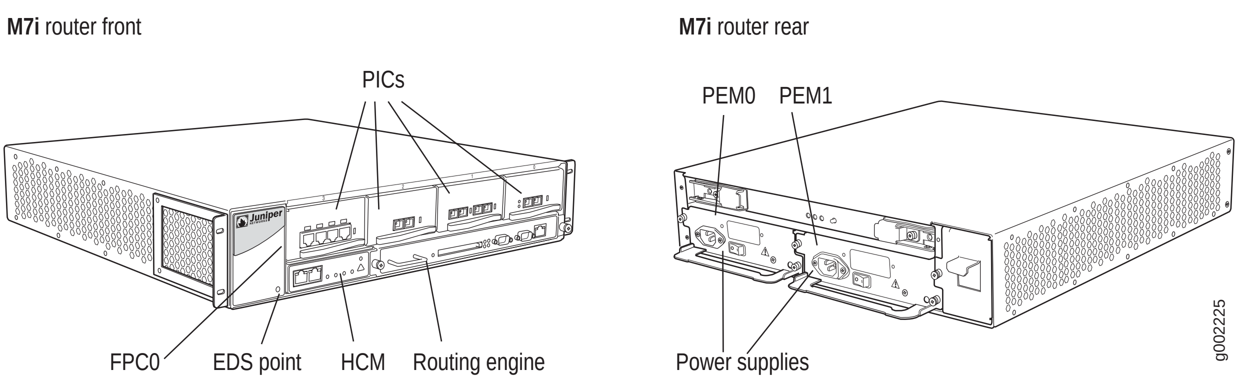


Figure 26 shows the front and rear of the M10i Internet router chassis and the installed components.

Figure 26: M10i Router Chassis and Components

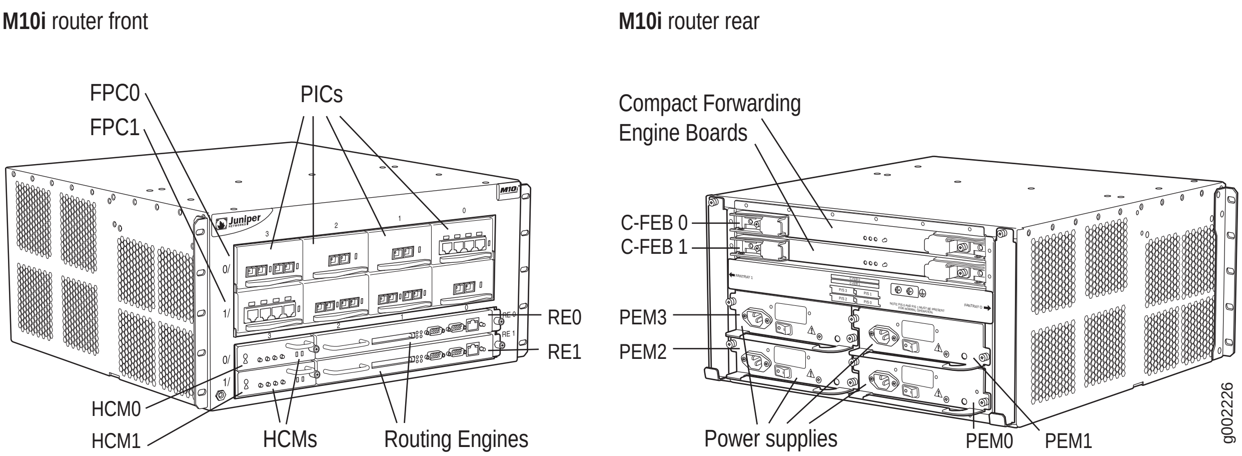


Figure 27 shows the front and rear of the M20 Internet router chassis and the installed components.

Figure 27: M20 Router Chassis and Components

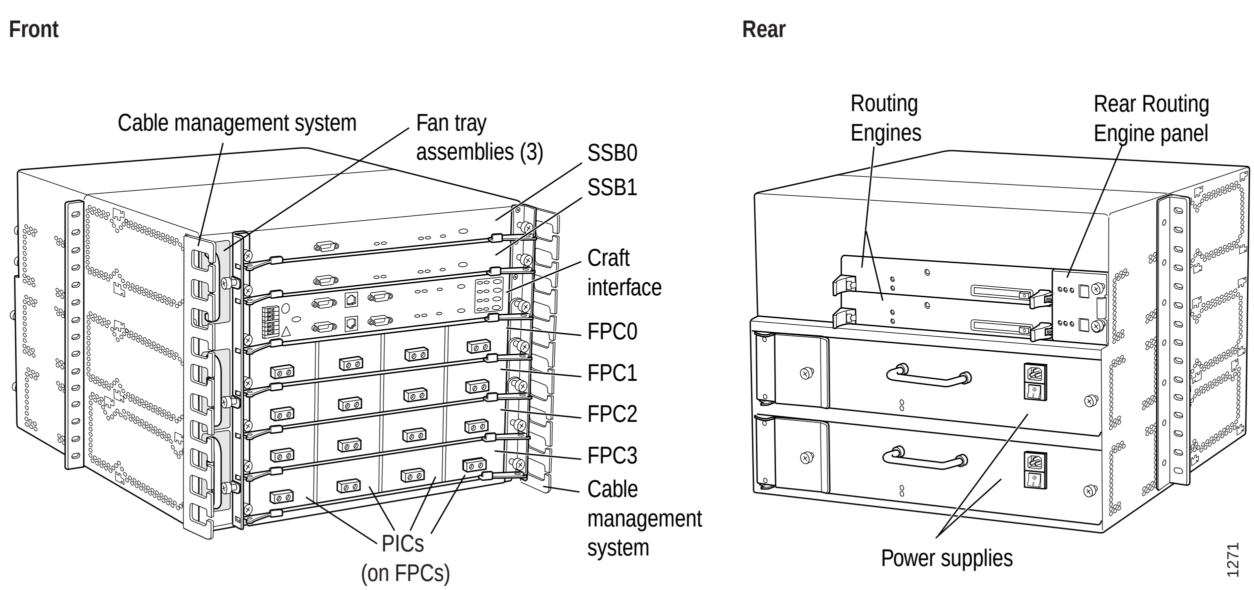


Figure 28 shows the front and rear of the M40 Internet router chassis and the installed components.

Figure 28: M40 Router Chassis and Components

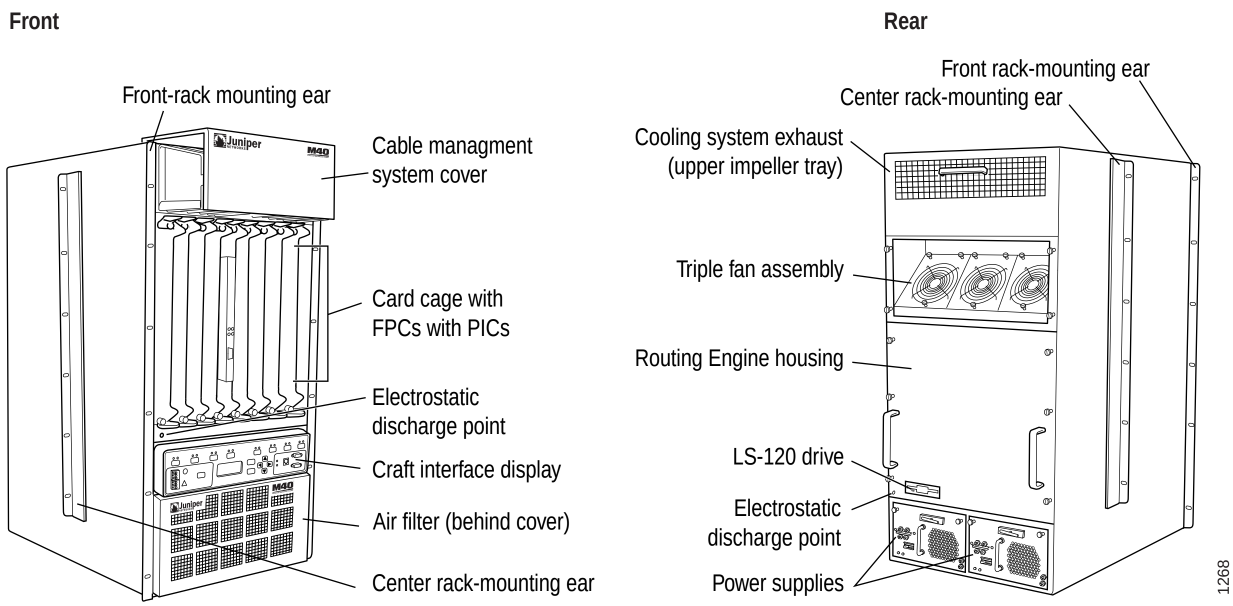


Figure 29 shows the front and rear of the M40e Internet router chassis and the installed components.

Figure 29: M40e Router Chassis and Components

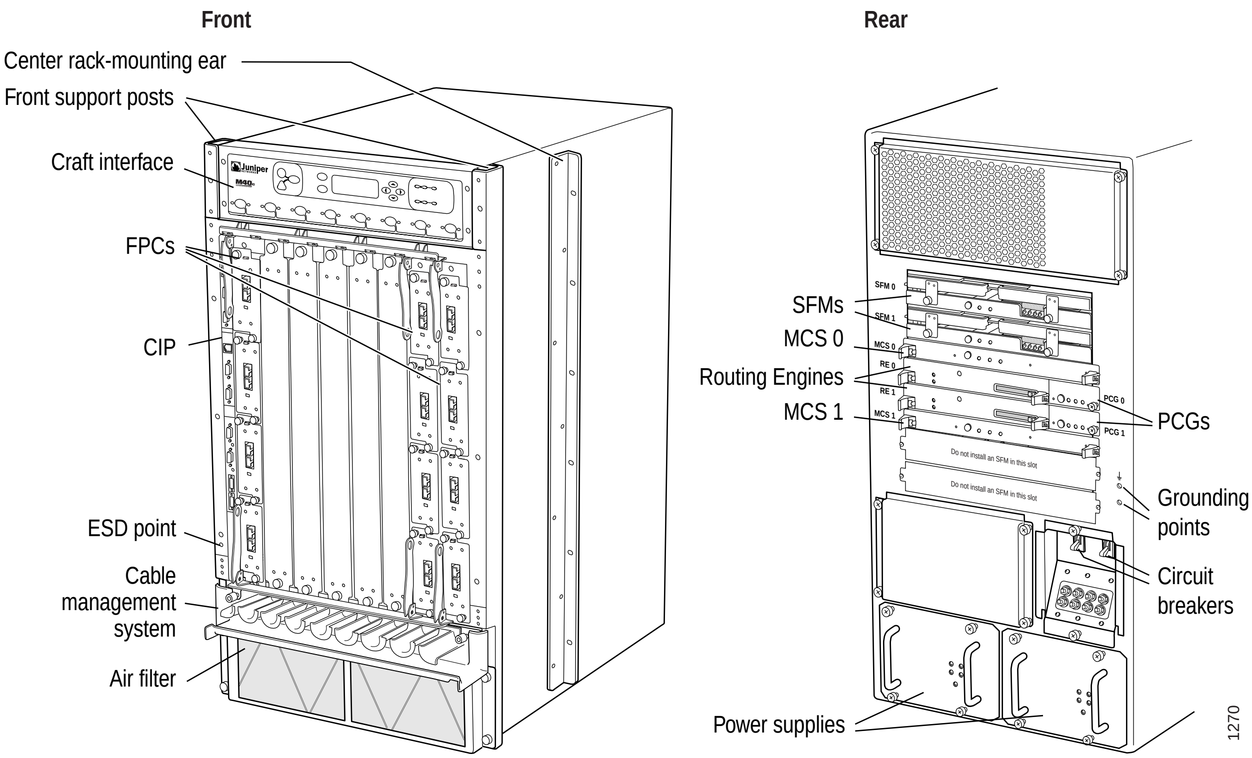


Figure 30 shows the front and rear of the M160 Internet router chassis and the installed components.

Figure 30: M160 Router Chassis and Components

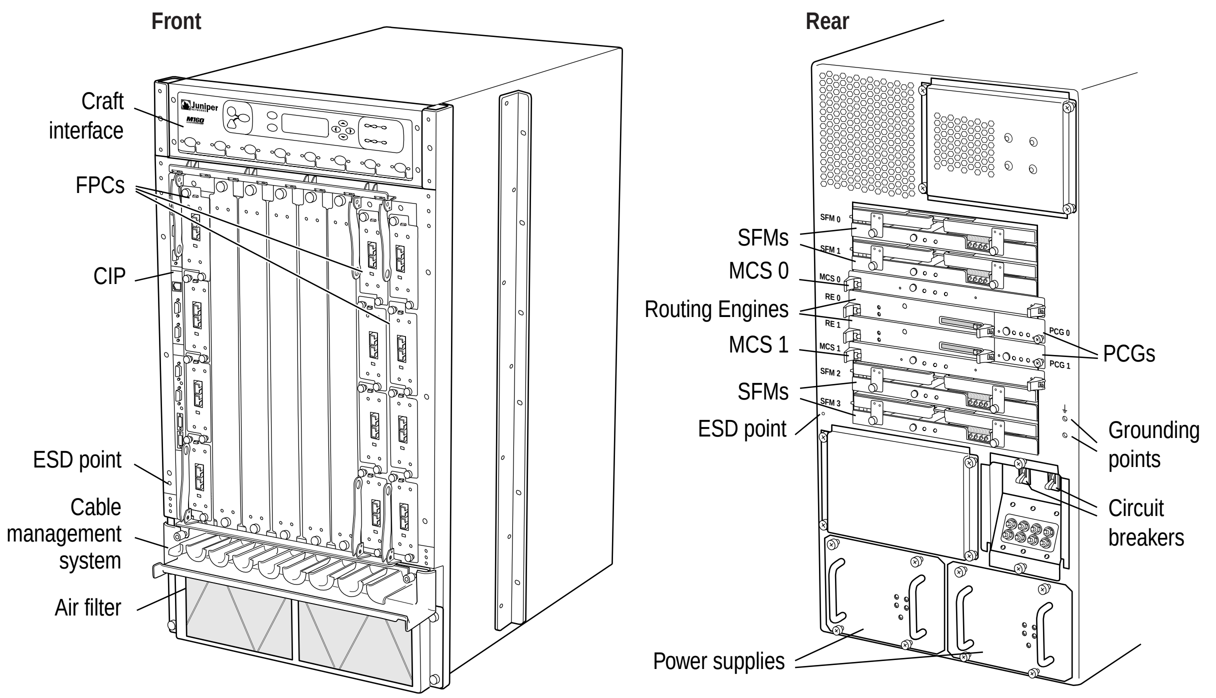


Figure 26 shows the front and rear of the M320 Internet router chassis and the installed components.

Figure 31: M320 Router Chassis and Components

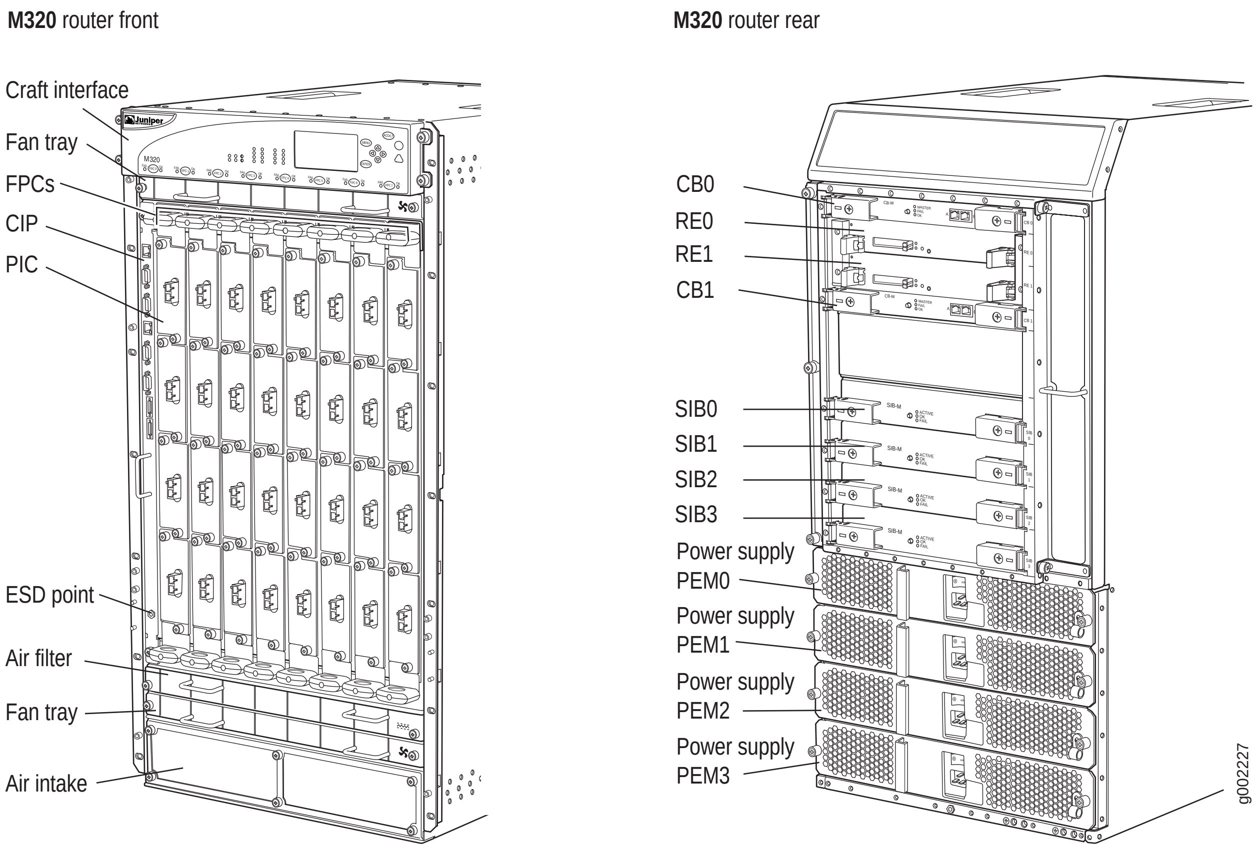


Figure 32 shows the front and rear of the T320 Internet router chassis and installed components.

Figure 32: T320 Router Chassis and Components

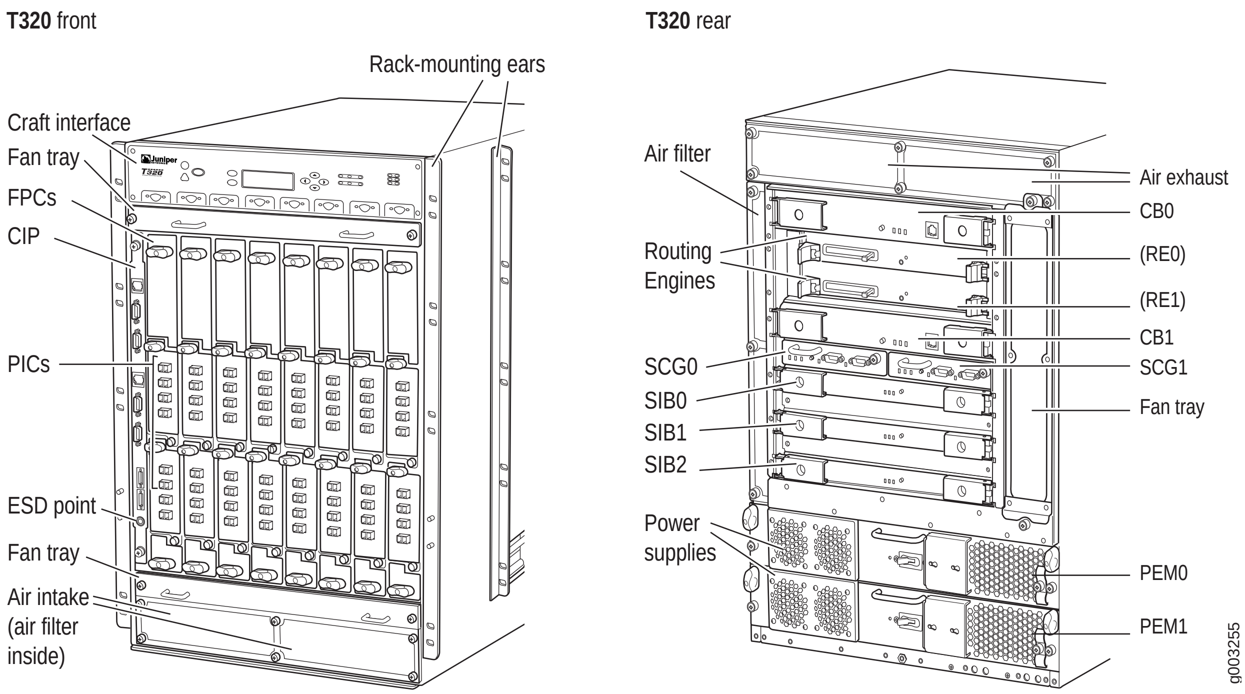
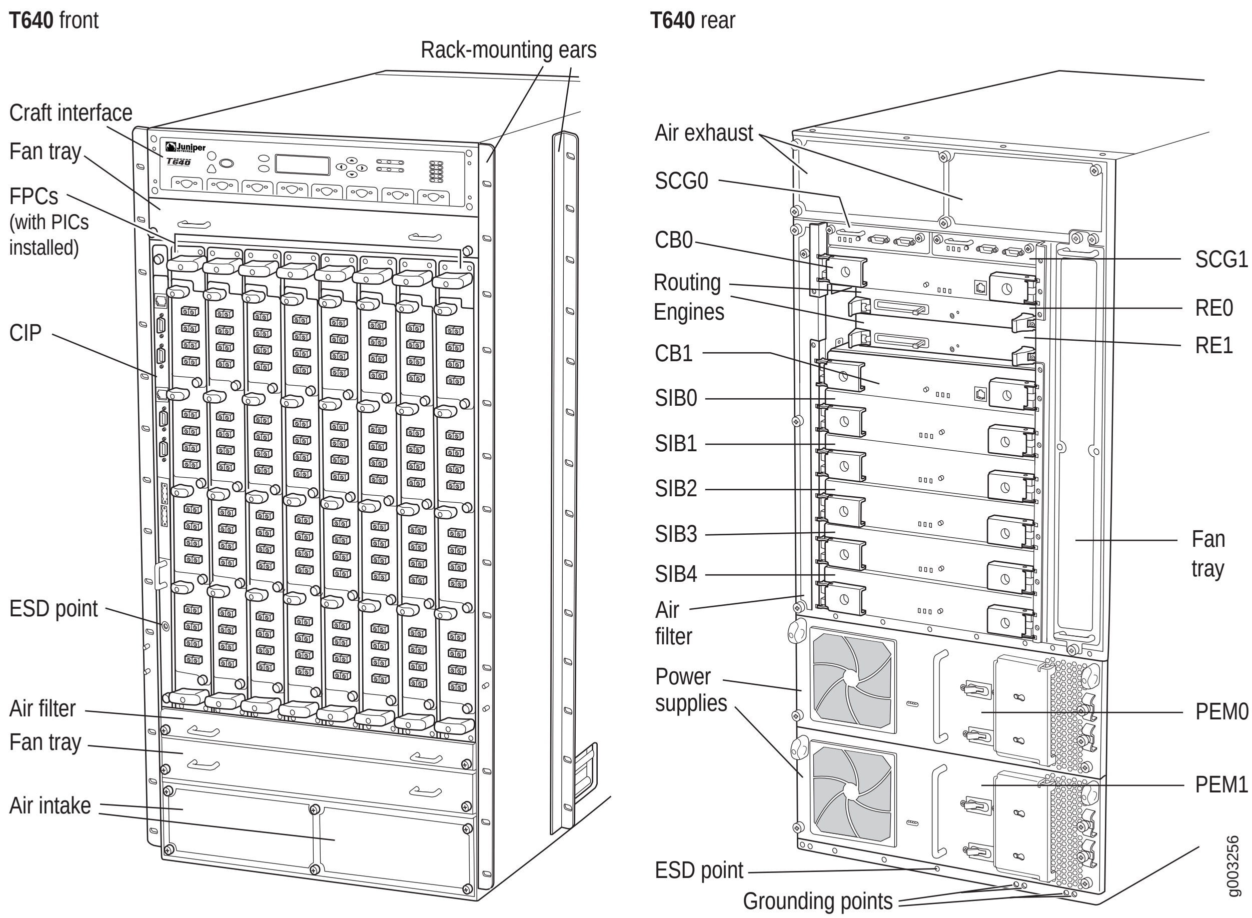


Figure 33 shows the front and rear of the T640 Internet routing node and the frinstalled components.

Figure 33: T640 Routing Node and Components



See Also

- M5 and M10 Internet Router Overview on page 3
- M7i Internet Router Overview on page 7
- M10i Internet Router Overview on page 11
- M20 Internet Router Overview on page 15
- M40 Internet Router Overview on page 19
- M40e Internet Router Overview on page 23
- M160 Internet Router Overview on page 27
- M320 Internet Router Overview on page 31

“T320 Internet Router Overview” on page 35

“T640 Internet Routing Node Overview” on page 39

Checking the Router Chassis Component Status

Steps To Take To check the status of the components installed in the router chassis, follow these steps:

1. Display the Hardware Components Installed in the Router Chassis on page 117
2. Check the Component Environmental Status on page 118
3. Check the Component Status from the Craft Interface on page 118

Step 1: Display the Hardware Components Installed in the Router Chassis

Action To display a list of the hardware components installed in the router chassis, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis hardware**

Sample Output

```
m160@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                101               M160
Midplane         REV 02   710-001245   S/N AB4107
FPM CMB          REV 01   710-001642   S/N AA2911
FPM Display      REV 01   710-001647   S/N AA2999
CIP              REV 02   710-001593   S/N AA9563
PEM 0            Rev 01   740-001243   S/N KJ35769       DC
PEM 1            Rev 01   740-001243   S/N KJ35765       DC
PCG 0            REV 01   710-001568   S/N AA9794
PCG 1            REV 01   710-001568   S/N AA9804
Host 1                                 da000004f8d57001  Present
MCS 1            REV 03   710-001226   S/N AA9777
SFM 0 SPP        REV 04   710-001228   S/N AA2975
SFM 0 SPR        REV 02   710-001224   S/N AA9838        Internet Processor I
SFM 1 SPP        REV 04   710-001228   S/N AA2860
SFM 1 SPR        REV 01   710-001224   S/N AB0139        Internet Processor I
FPC 0            REV 03   710-001255   S/N AA9806        FPC Type 1
  CPU            REV 02   710-001217   S/N AA9590
  PIC 1          REV 05   750-000616   S/N AA1527        1x OC-12 ATM, MM
  PIC 2          REV 05   750-000616   S/N AA1535        1x OC-12 ATM, MM
  PIC 3          REV 01   750-000616   S/N AA1519        1x OC-12 ATM, MM
FPC 1            REV 02   710-001611   S/N AA9523        FPC Type 2
  CPU            REV 02   710-001217   S/N AA9571
  PIC 0          REV 03   750-001900   S/N AA9626        1x STM-16 SDH, SMIR
  PIC 1          REV 01   710-002381   S/N AD3633        2x G/E, 1000 BASE-SX
FPC 2                                                    FPC Type OC192
  CPU            REV 03   710-001217   S/N AB3329
  PIC 0          REV 01                                  1x OC-192 SM SR-2
```

What It Means The command output displays a list of the components installed in the M160 router chassis, including the name, revision level, part number, serial number, and a brief description of the component. From this output, you can determine which components to maintain and monitor to ensure optimum router operation. The command output is similar for other routers.

Step 2: Check the Component Environmental Status

Action To check the environmental status of the router component, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
m20@host> show chassis environment
Class Item                  Status     Measurement
Power Power Supply A        OK
      Power Supply B        OK
Temp  FPC Slot 1            OK         30 degrees C / 86 degrees F
      FPC Slot 2            OK         29 degrees C / 84 degrees F
      Power Supply A        OK         23 degrees C / 73 degrees F
      Power Supply B        OK         21 degrees C / 69 degrees F
      SSB Slot 0            OK         30 degrees C / 86 degrees F
      Backplane             OK         24 degrees C / 75 degrees F
Fans  Rear Fan              OK         Spinning at normal speed
      Upper Fan             OK         Spinning at normal speed
      Middle Fan            OK         Spinning at normal speed
      Bottom Fan            OK         Spinning at normal speed
Misc  Craft Interface       OK
```

What It Means The command output lists the components installed in an M20 router chassis, including the category or class, component name, operational status, and temperature or speed measurement. Use this command to get a quick status of each component installed in the router chassis. You can also use the show chassis *component-name* CLI command to get more detailed status information on certain components for isolating problems. For an example, see “Display Detailed Component Environmental Information” on page 59.

Step 3: Check the Component Status from the Craft Interface

Action To check the router operation status from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
m160@host> show chassis craft-interface
FPM Display contents:
    +--------------------+
    |myrouter            |
    |Up: 1+16:46         |
    |                    |
    |Fans OK             |
    +--------------------+

Front Panel System LEDs:
Host     0    1
------------------------
OK       .    *
Fail     .    .
Master   .    *

Front Panel Alarm Indicators:
-----------------------------
Red LED      .
Yellow LED   .
Major relay  .
```

```
Minor relay  .

Front Panel FPC LEDs:
FPC    0   1   2   3   4   5   6   7
------------------------------------
Red    .   .   .   .   .   .   .   .
Green  *   *   .   .   .   .   .   .

MCS and SFM LEDs:
MCS    0   1      SFM    0   1   2   3
--------------------------------------
Amber      .             .   .
Green      .             .   .
Blue       *             *   *
```

What It Means The command output displays the router system operation status for an M160 router, including the alarm indicators, the information displayed on the craft interface LCD display, and the component LEDs. An asterisk (*) indicates that the component is operating normally. A dot is merely a placeholder, and indicates nothing. For example, the asterisks in the Host Front Panel System LEDs section indicate that the Routing Engine in slot 1 is operating normally and that it is the master. The dots in the Front Panel Alarm Indicators section indicate that there are no system alarms.

Alternative Actions Physically look at the router craft interface. The router name in the LCD display helps verify that you have located the correct router to monitor. For more information about the craft interface, see “Monitoring the Craft Interface” on page 197 or the appropriate router hardware guide.

Checking Router Alarms

Chassis alarms indicate a problem with a chassis component, such as the Flexible PIC Concentrators (FPCs), cooling system, power supplies, and other components. For a listing of the chassis alarms for a particular router, see the appropriate router hardware guide.

For information about conditions that trigger router component alarms, see:

- “M5 or M10 Router Chassis Component Alarm Conditions” on page 61
- “M7i or M10i Router Chassis Component Alarm Conditions” on page 63
- “M20 Router Chassis Component Alarm Conditions” on page 65
- “M40 Router Chassis Component Alarm Conditions” on page 68
- “M40e or M160 Router Chassis Component Alarm Conditions” on page 71
- “M320 Router Chassis Component Alarm Conditions” on page 74
- “T320 Router Chassis Component Alarm Conditions” on page 77
- “T640 Routing Node Chassis Component Alarm Conditions” on page 80

Steps To Take

To check router system alarms, follow these steps:

1. Display Current Component Alarms on page 120
2. Display Component Error Messages in the System Log File on page 121

Step 1: Display Current Component Alarms

Action

To display the active chassis alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
5 alarms are currently active

Alarm time              Class Description

 2002-04-16 15:09:01 PDT Major PIC 2/2 failed to initialize
 2002-04-16 15:08:40 PDT Major Power Supply A 2.5 volt output failed
 2002-04-16 15:08:40 PDT Major Power Supply A 5 volt output failed
 2002-04-16 15:08:40 PDT Major Power Supply A 3.3 volt output failed
 2002-04-16 15:08:40 PDT Major Power Supply A fan failed
```

What It Means

The command output displays the number of alarms currently active, the time at which the alarm began, the severity level, and an alarm description. Note the date and time of an alarm so that you can correlate it with error messages in the messages system log file. This sample command output is for a router from which the lower fan tray and the power supply have been removed, and the management Ethernet interface disconnected. The craft interface display, in alarm mode, displays a short description of the alarm. The show chassis alarms command output displays a longer description of the alarm.

Alternative Actions

To view active router alarms, you can physically look at the craft interface or use the show chassis craft-interface command.

The show chassis craft-interface command displays the most severe alarm first, the alarm indicator status, and the number of active alarms. You cannot scroll through the alarms (if there are more than two) at the command line.

```
user@host> show chassis craft-interface
Red alarm:     LED on, relay on
Yellow alarm:  LED off, relay off
Host OK LED:   On
Host fail LED: Off

FPCs     0  1  2  3
-------------------
Green    *  *  *  *
Red      .  .  .  .

LCD screen:
     +--------------------+
     |myrouter            |
     |5 Alarms active     |
     |R: PIC 2/2 FAILED   |
     |R: Supply A 2v FAIL |
     +--------------------+
```

When a red or yellow alarm occurs, the craft interface goes into alarm mode. Alarm mode preempts idle mode, displaying a message to alert you of serious alarm conditions. In alarm mode, the screen displays the following information:

- First line—Name of the router.
- Second line—Number of alarms active on the router.
- Third and fourth lines—Individual alarms, with the most severe condition shown first. Each line indicates whether the alarm is red (R) or yellow (Y).

For more information about the craft interface, see “Monitoring the Craft Interface” on page 197 or the appropriate router hardware guide.

Step 2: Display Component Error Messages in the System Log File

Action To display component error messages in the messages system log file, use the following JUNOS CLI operational mode command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
[...Output truncated...]
Apr 17 11:12:45 tylenol scb CM: ALARM SET: (Major) Power Supply B fan failed
Apr 17 11:12:46 tylenol scb CM: ALARM CLEAR: Power Supply B fan failed
Apr 17 11:12:46 tylenol alarmd[590]: Alarm cleared: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply B fan failed
Apr 17 11:13:09 tylenol alarmd[590]: Alarm set: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply B fan failed
Apr 17 11:13:09 tylenol scb CM: ALARM SET: (Major) Power Supply B fan failed
Apr 17 11:13:10 tylenol alarmd[590]: Alarm cleared: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply B fan failed
Apr 17 11:13:10 tylenol scb CM: ALARM CLEAR: Power Supply B fan failed
[...Output truncated...]
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can use the date and time to browse the messages log file, or you can use the show log messages | match *component-name* command to view error messages that are specific to a particular component. For example, the command output shows the common power supply error messages logged from the router. In the filter expression, if there is a space in the component name, enclose the component name in quotation marks, for example | match “power supply”.

Use system log file information to isolate a component problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated at the time of the event. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display Component Errors in the Chassis Daemon Log File

Action To display component error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jun 11 20:45:08 *** inventory change ***
Jun 11 20:45:08 CIP set alarm 0x1
Jun 11 20:45:08 alarm op fru 34 op 1 reason 1
Jun 11 20:45:08 send: red alarm set, class 100 obj 112 reason 1
Jun 11 20:45:08 CIP removed
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is maintained when components are added or removed. The command output displays error messages that are generated when a Connector Interface Panel (CIP) fails or is removed.

Verifying Router Component Failure

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the component for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To verify router component failure, perform a swap test on a component as follows:

1. Replace a failed component with one that you know works.

2. Verify the component status by using the appropriate show chassis *component-name* command. If the replaced component works, the original component is defective.

3. If the replaced component does not work, remove it and check the component midplane connector for bent pins. If the replaced component still does not work, contact JTAC, and see "Return the Failed Component" on page 86.

Replacing a Failed Component

Action To return the router chassis, you need to know the chassis serial number. To display the midplane serial number, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
m160@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                101               M160
Midplane         REV 02   710-001245   S/N AB4107
FPM CMB          REV 01   710-001642   S/N AA2911
FPM Display      REV 01   710-001647   S/N AA2999
[...Output truncated...]
```

What It Means

The chassis serial number is AB4107.

To return a chassis, see “Return the Failed Component” on page 86. See also the appropriate router hardware guide.

Chapter 14

Monitoring the Routing Engine

You monitor and maintain the Routing Engine, a key router component, to ensure that all system processes function normally, including routing protocols, packet forwarding tables, router interfaces, system management, JUNOS software and file system storage, and monitoring functions. (See Table 31.)

Table 31: Checklist for Monitoring the Routing Engine

Monitor Routing Engine Tasks	Command or Action
Understanding the Routing Engine on page 127	
■ Routing Engine Types and Characteristics on page 127 ■ Routing Engine Locations on page 130 ■ Routing Engine Redundancy on page 135 ■ Routing Engine Component Companionship on page 135 ■ Routing Engine Boot Devices on page 135 ■ Routing Engine Storage Media on page 136	
Monitoring the Routing Engine Status on page 136	
1. Check the Detailed Routing Engine Status on page 137	show chassis routing-engine show chassis environment routing-engine
2. Check the Routing Engine LEDs on page 138	■ Check the M7i Routing Engine LEDs on page 139 ■ Check the M20 Router Routing Engine LEDs on page 140 ■ Check the M40 Router Routing Engine LEDs on page 142 ■ Check the M40e and M160 Router Routing Engine LEDs on page 143 ■ Check the M320 Router Routing Engine LEDs on page 144 ■ Check the T320 Router Routing Engine LEDs on page 144 ■ Check the T640 Routing Node Routing Engine LEDs on page 145
3. Check the Redundant Routing Engine Status from the Craft Interface CLI Output on page 146	show chassis craft-interface
Verifying Routing Engine Failure on page 149	
1. Check Core Files If the Routing Engine Reboots on page 149	■ List the Core Files Generated After A Crash Occurs on page 149 ■ Display the Messages Log File After A Crash Occurs on page 150 ■ Example of When No Core File Is Generated on page 150

Monitor Routing Engine Tasks	Command or Action
2. Example of Boot Messages If Routing Engine Fails to Boot on page 150	show system storage show system boot-messages show log messages
3. Check for Compact Flash Media and Hard Disk Failure on page 150	■ When the Compact Flash Is Removed from the Boot List on page 151 ■ Determine Why Compact Flash Did Not Mount on page 151 ■ When the Hard Disk Is Removed from the Boot List on page 152 ■ Verify That the Hard Disk Did Not Mount on page 152 ■ Verify That the Hard Disk Is Missing from The Boot List on page 153 ■ View Alarms When Media Is Removed from the Boot List on page 153
4. Understand What Happens When Memory Failures Occur on page 154	
5. Check the Router File System and Boot Disk on page 154	show system storage
6. Display the Current Routing Engine Alarms on page 155	show chassis alarms
7. Display Error Messages in the System Log File on page 155	show log messages
8. Document the Events Prior to the Failure on page 156	Write down failure events as they occur. Turn on logging on your system console.
Getting Routing Engine Hardware Information on page 157	
1. Display Routing Engine Hardware Information on page 157	show chassis hardware
2. Locate the Routing Engine Serial Number ID Label on page 158	Locate the Routing Engine serial number ID label. If you see two serial numbers, give both to JTAC.
Removing a Routing Engine on page 161	The Routing Engine is hot-pluggable. Follow the procedures in the applicable router hardware guide. **Note:** The M5/M10 routers have a cover over the Routing Engine. The M40e and M160 routers have a cover over all the rear chassis components. Remember to remove the screws (M5/M10, M20, M40e, and M160 routers) or captive screws (T320 router and T640 routing node) next to the ejector clips before you remove the Routing Engine.

Understanding the Routing Engine

Purpose Inspect the Routing Engine to ensure that key system processes are operating normally.

What Is a Routing Engine The Routing Engine is a key component in the router. It is primarily responsible for the protocol intelligence of the router. Thus, it is responsible for creating a routing table, which consists of all routes learned by all protocols running on the router. The Routing Engine interprets the routing table, generates a subset of routes to be used for all forwarding purposes, and places them in the forwarding table. The Routing Engine also holds the microcode for the Packet Forwarding Engine.

The Routing Engine is responsible for user interaction functions, such as the command-line interface (CLI), Simple Network Management Protocol (SNMP) management, and craft interface interaction.

The Routing Engine consists of the following components:

- Intel Pentium compact Peripheral Component Interconnect (PCI) platform
- Nonrotating compact flash drive (RAM disk)
- Standard rotating hard drive
- Removable media drive

The JUNOS software resides on the compact flash drive, with an alternate copy residing on the system hard drive.

This section also includes the following information:

- Routing Engine Types and Characteristics on page 127
- Routing Engine Locations on page 130
- Routing Engine Redundancy on page 135
- Routing Engine Component Companionship on page 135

Routing Engine Types and Characteristics

This section lists the Routing Engine characteristics that are supported in each routing platform. It also shows the Routing Engine component supported in each routing platform. This section covers the following routing platforms:

- M7i and M10i Router Routing Engine on page 128
- M5, M10, M20, M40, M40e, and M160 Router Routing Engines on page 129
- M320 Router Routing Engine on page 129
- T320 Router and T640 Routing Node Routing Engine on page 130

Table 32 lists the Routing Engine type characteristics for each routing platform.

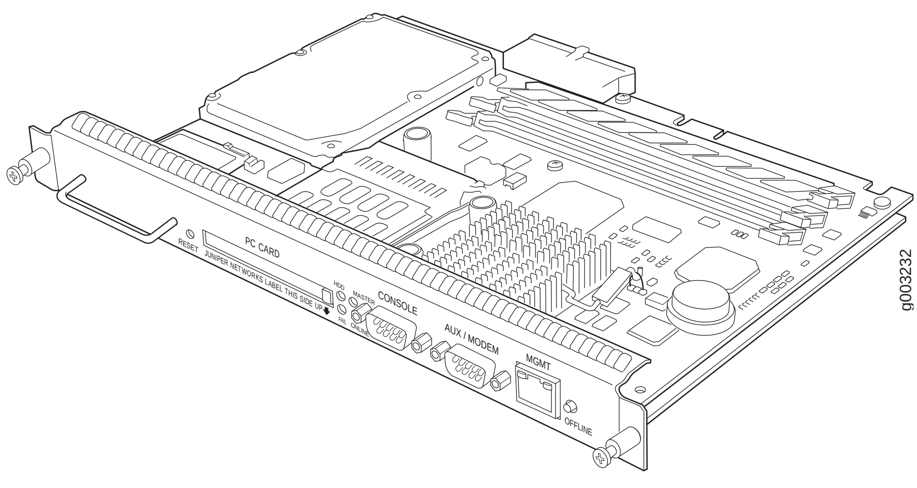
Table 32: Routing Engine Characteristics Per Routing Platform

Routing Engine	CLI Name	Processor	Memory	Hard Drive	Routing Platforms
RE-M40 (RE-200)	RE1	Intel Pentium 200 MHz	256 MB	6.4 GB	M40
RE-333 – 768	RE2	Intel Pentium2 333 MHz	768 MB 256 MB (M5, M10)	10 – 20 GB	M5, M10, M20, M40 (requires new housing)
RE-600 – 2048	RE3	Intel Pentium3 600 HHz	2048 MB	30 GB	M5, M10, M20, M40, M40e, M160, T320, T640
RE-1600 – 2048	RE4	Intel Pentium4 1.6 GHz	2048 MB	30 GB	M320, T320, T640
RE-400 – 256 + 512 Upgrade	RE5	Intel Celeron 400 MHz	768 MB	20 GB	M7i, M10i

M7i and M10i Router Routing Engine

Figure 34 shows the Routing Engine that is supported in the M7i and M10i routing platforms. For the current Routing Engines supported on these routing platforms, see Figure 32.

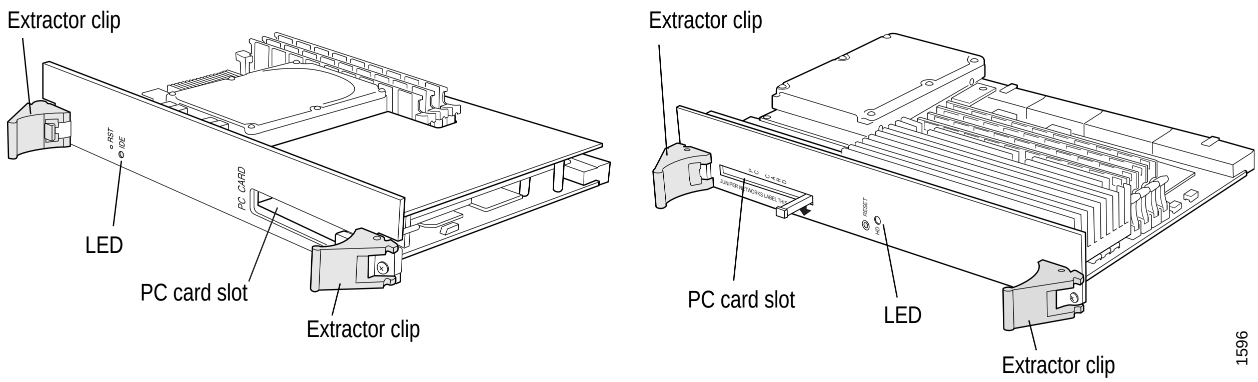
Figure 34: M7i and M10i Router Routing Engine



M5, M10, M20, M40, M40e, and M160 Router Routing Engines

Figure 35 shows the Routing Engines that are supported in the M5, M10, M20, M40, M40e, and M160 routing platforms. For the current Routing Engines supported on these routing platforms, see Figure 32 on page 128.

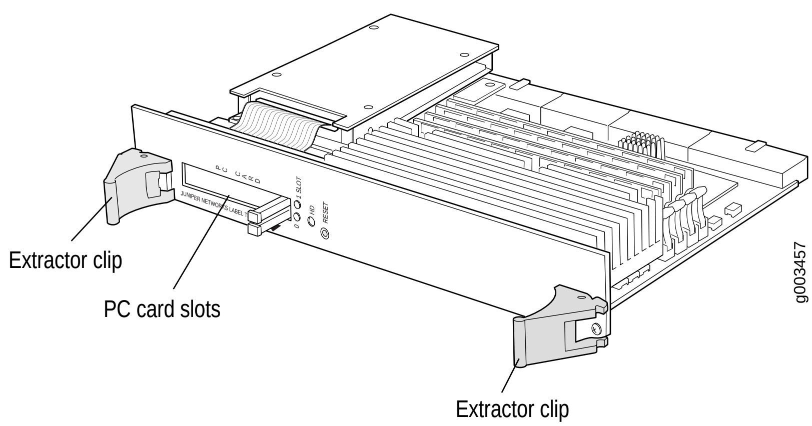
Figure 35: M5, M10, M20, M40, M40e, and M160 Router Routing Engines



M320 Router Routing Engine

Figure 36 shows the Routing Engine that is supported in the M320 routing platform. For the current Routing Engines supported on these routing platforms, see Figure 32 on page 128.

Figure 36: M320 Router Routing Engine



T320 Router and T640 Routing Node Routing Engine

Figure 37 shows the Routing Engine that is supported in the M320 routing platform. For the current Routing Engines supported on these routing platforms, see Figure 32 on page 128.

Figure 37: T320 Router and T640 Routing Node Routing Engine

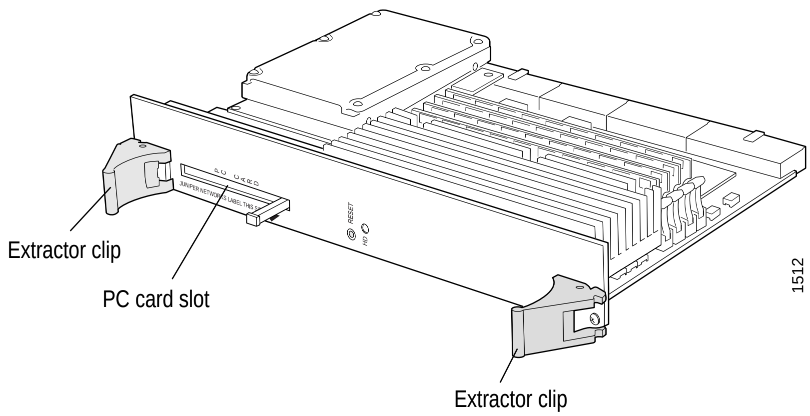


Figure 38 shows the Routing Engine location in the M5, M10, and M20 Internet routers.

Routing Engine Locations

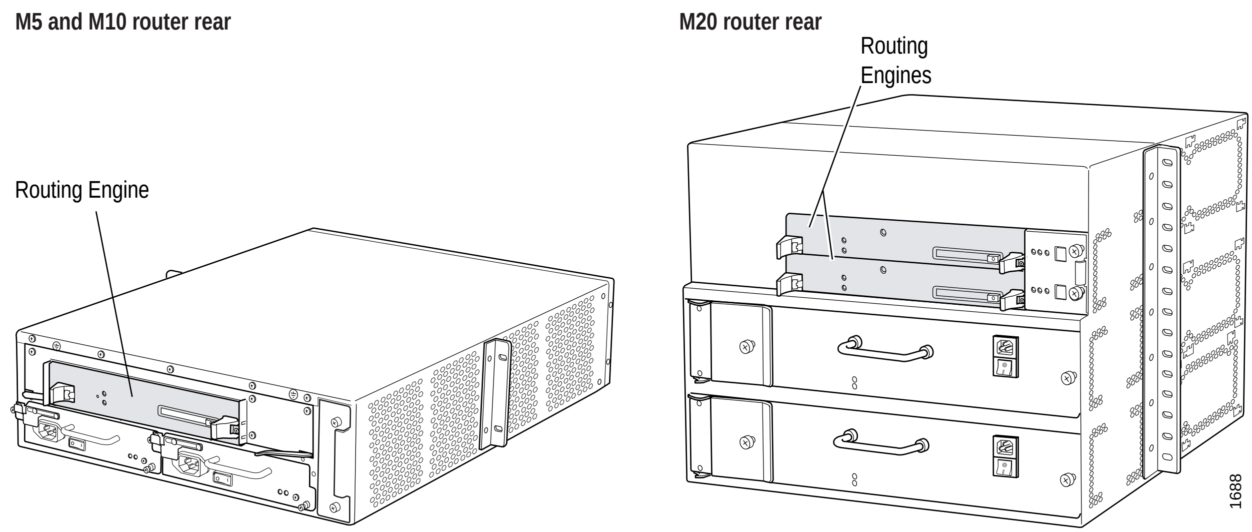
This section shows where the Routing Engines are installed in each Routing Platform. This section includes the following locations:

- M5, M10, and M20 Router Routing Engines Location on page 131
- M7i and M10i Router Routing Engine Location on page 131
- M40 Router Routing Engine Location on page 132
- M40e and M160 Router Routing Engine Location on page 133
- M320 Router Routing Engine Location on page 134
- T320 Router and T640 Routing Node Routing Engine Location on page 134

M5, M10, and M20 Router Routing Engines Location

Figure 38 shows the Routing Engine location in the M5, M10, and M20 routing platforms.

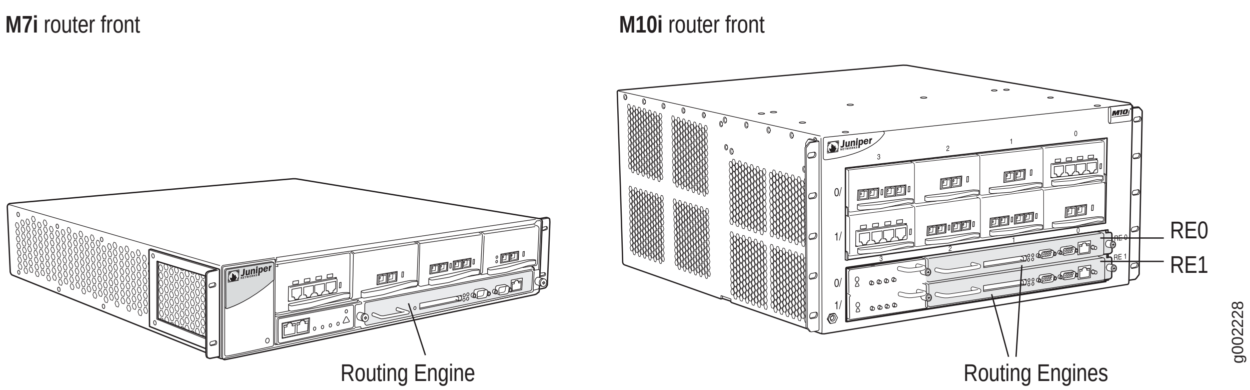
Figure 38: M5, M10, and M20 Router Routing Engine Location



M7i and M10i Router Routing Engine Location

Figure 39 shows the Routing Engine location in the M7i and M10i routers.

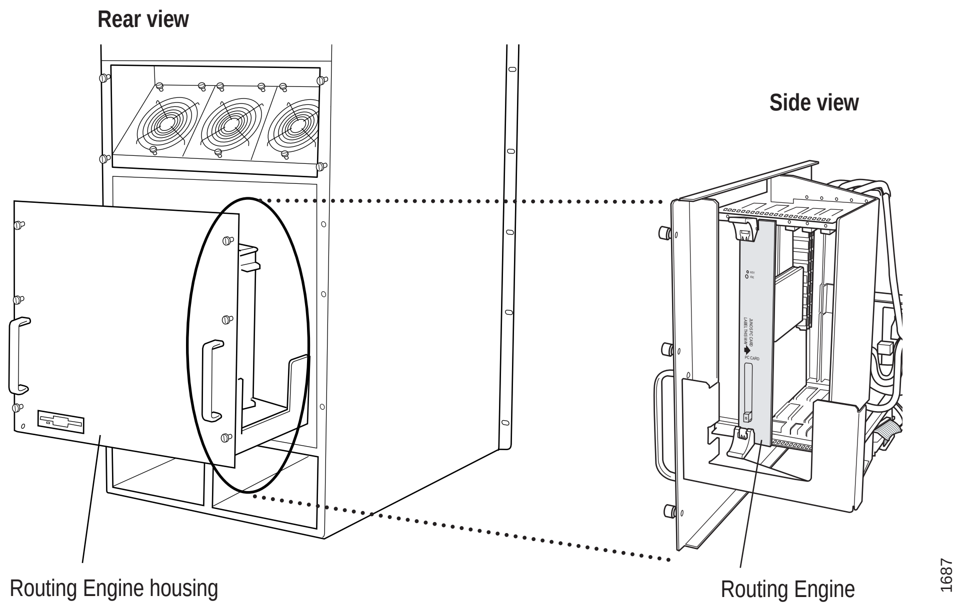
Figure 39: M7i and M10i Router Routing Engine Location



M40 Router Routing Engine Location

Figure 40 shows the location of the Routing Engine on the M40 router.

Figure 40: M40 Router Routing Engine Location



On the M40 Internet router, the Routing Engine module resides in a metal housing at the back of the chassis, below the fans, in a compartment behind the card cage (see Figure 40).

The M40 router supports three Routing Engine models: RE-M40 (RE1), RE-333 (RE2), and RE-600 (RE3). See Table 32 on page 128.

All M40 routers shipped before mid-2001 had RE-M40 Routing Engines. All M40 routers shipped after mid-2001 have the RE-333 Routing Engine and housing. You could also upgrade to the RE-600 (RE3) Routing Engine.

The RE-333 and the RE-600 Routing Engines share the same housing, which is different from the RE-M40. Therefore, if you want to upgrade from an RE-M40 to an RE-333 or RE-600, you must also upgrade the Routing Engine housing.

NOTE: Effective July 15, 2001, the RE-M40 Routing Engine was replaced by the RE-333 Routing Engine, which was made available with JUNOS software, release 4.2. After July 15, 2004, the RE-M40 Routing Engine is no longer supported. See "Routing Engine Characteristics Per Routing Platform" on page 128.

See also the End-of-sale and End-of-service Announcement for the M40 routing platform and products at https://www.juniper.net/support/eol/.

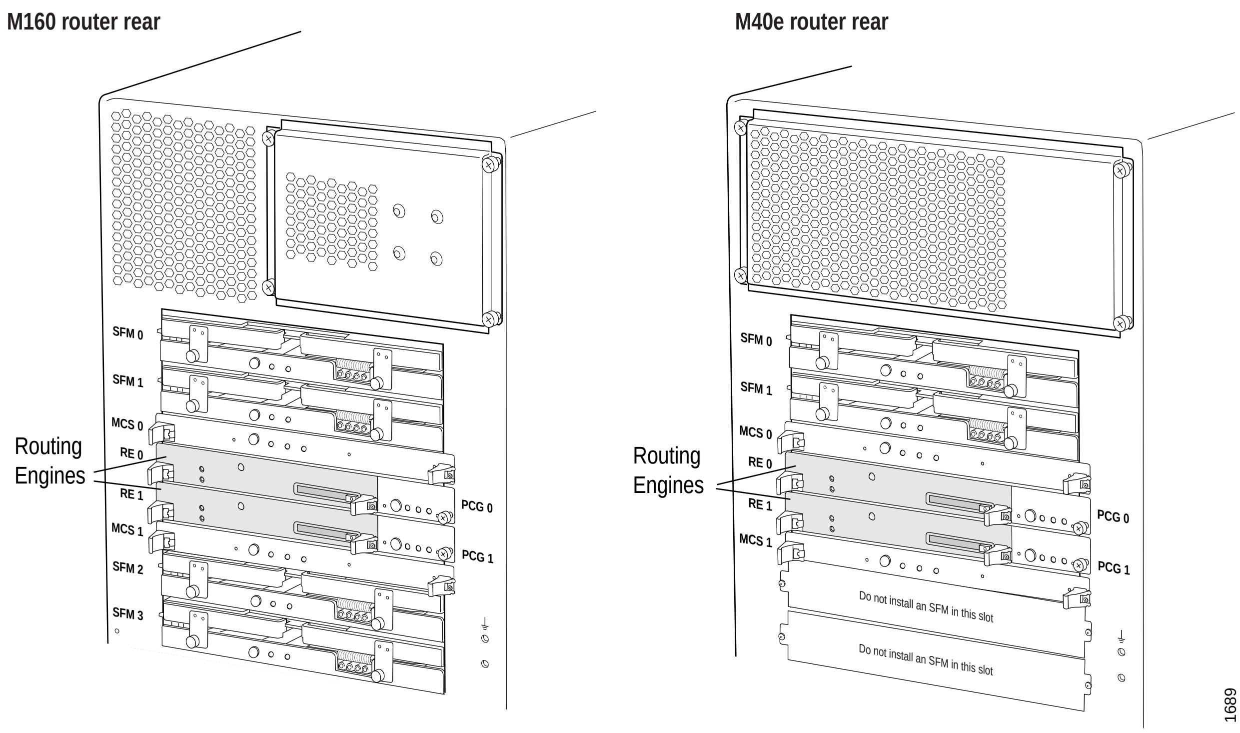
If you upgrade the Routing Engine housing, the PCMCIA card slot is not accessible and you must use the LS-120 PC card. If you want to install a new version of the JUNOS software, you must use the LS-120 drive.

You can replace the entire Routing Engine housing or just the Routing Engine.

M40e and M160 Router Routing Engine Location

Figure 41 shows the Routing Engine location on the M40e and M160 router.

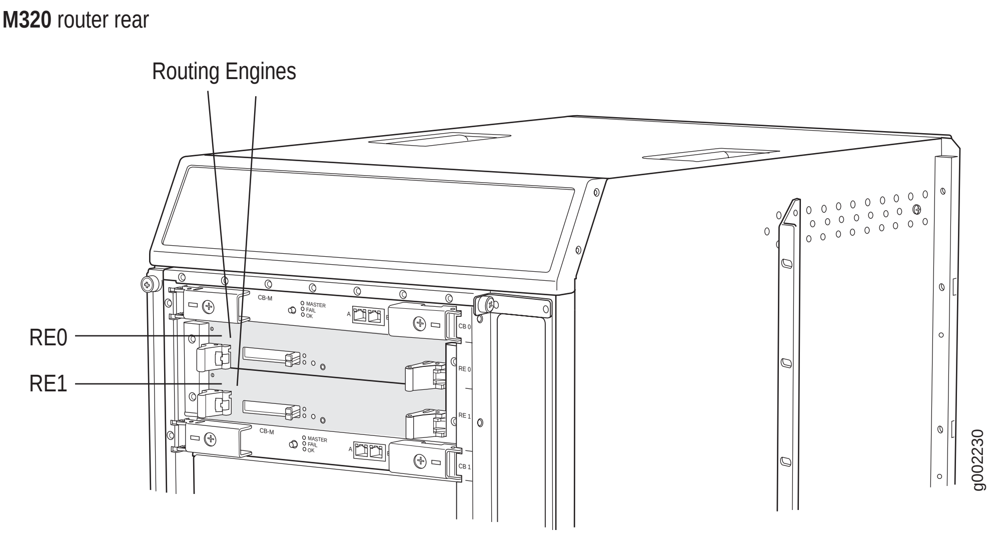
Figure 41: M40e and M160 Router Routing Engine Location



M320 Router Routing Engine Location

Figure 42 show the Routing Engine location on the M320 Internet router.

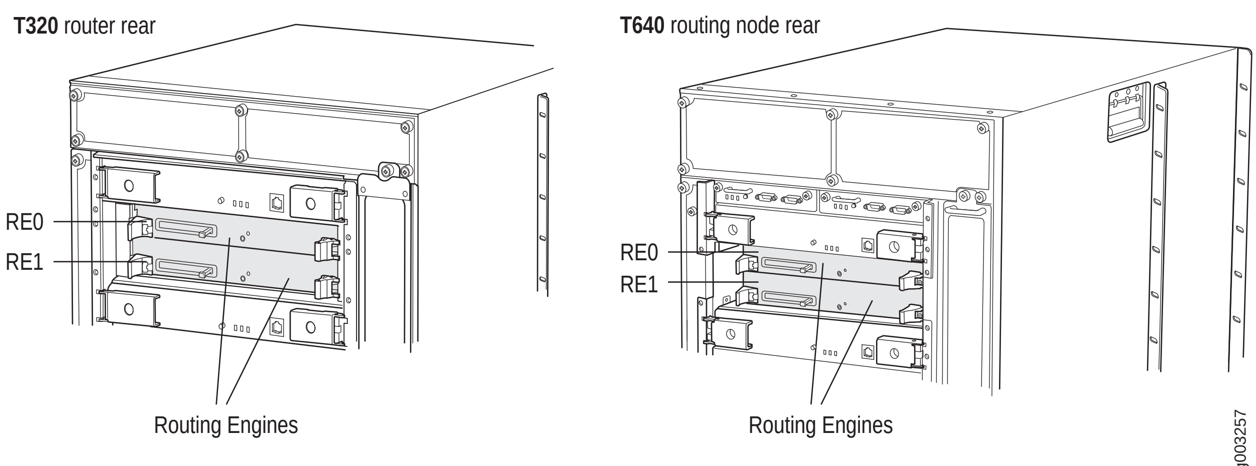
Figure 42: M320 Router Routing Engine Location



T320 Router and T640 Routing Node Routing Engine Location

Figure 43 shows the Routing Engine location on the T320 router and T640 routing node.

Figure 43: T320 Router and T640 Routing Node Routing Engine Location



Routing Engine Redundancy

Table 33 show the routing platforms that can have redundant Routing Engines. See "Routing Engine Component Companionship" on page 135.

Table 33: Redundant Routing Engines

Characteristic	M5/ M10	M7i	M10i	M20	M40	M40e/M160	M320/T320/ T640
Redundant Routing Engines			X works with HCM	X		X (Host Module) works with MCS	X (Host Subsystem) works with Control Board

Routing Engine Component Companionship

On the M10i router, the Routing Engine works with its companion High-Availability Chassis Manager (HCM) to provide control and monitoring functions for router components. For more information about the HCM, see "Monitoring the HCM" on page 431. For more information about monitoring Redundant HCMs, see "Monitoring Redundant HCMs" on page 623.

For information about monitoring redundant Routing Engines, see "Host Redundancy Overview" on page 463 and "Monitoring Redundant Routing Engines" on page 491.

On the M40e and M160 routers, the host module provides the routing and system management functions. The host module consists of the Routing Engine and the Miscellaneous Control Subsystem (MCS). For more information about the host module, see "Monitoring the Host Module" on page 341. For more information about the MCS, see "Monitoring the MCS" on page 359.

On the M320 router, T320 router, and T640 routing node, the host subsystem provides the routing and system management functions. The host subsystem consists of the Routing Engine and the Control Board. For more information about the host subsystem, see "Monitoring the Host Subsystem" on page 289. For information about the Control Boards, see "Monitoring the Control Board" on page 301.

For more detailed information about the Routing Engine, see the appropriate router hardware guide.

Routing Engine Boot Devices

Generally the router boots on the primary boot device, which is the flash disk. This device contains the current router configuration and the last three committed configurations in the juniper.conf, juniper.conf.1.gz, juniper.conf.2.gz, and juniper.conf.3.gz files, respectively. These files are located in the /config directory.

If the flash disk fails, the router attempts to boot from the hard disk, which is the alternate boot device.

If a removable media is installed when the router boots, the router attempts to boot the image on it. If the booting fails, the router tries the flash drive and then the hard disk.

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

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

— JUNOS 6.4 R1 built date
—
— NOTICE: System is running on alternate media device (/dev/ad1).
```

Routing Engine Storage Media

The router has three forms of storage media:

- Flash drive, which is a nonrotating drive. When a new router is shipped from the factory, the JUNOS software is preinstalled on the flash drive.
- Hard disk, which is a rotating drive. When a new router is shipped from the factory, the JUNOS software is preinstalled on the hard disk. This drive is also used to store system log files and diagnostic dump files.
- Removable media, either a PC card or an LS-120 floppy disk. The removable media that ships with each router contains a copy of the JUNOS software.

Table 43 on page 154 shows the storage media device names (as of JUNOS release 5.x and above) by Routing Engine type.

See Also

- "Host Redundancy Overview" on page 463
- "Monitoring Redundant Routing Engines" on page 491

Monitoring the Routing Engine Status

For information about conditions that trigger Routing Engine alarms, see "Display the Current Router Alarms" on page 61.

Steps To Take

To monitor the Routing Engine status, follow these steps:

1. Check the Detailed Routing Engine Status on page 137
2. Check the Routing Engine LEDs on page 138

Step 1: Check the Detailed Routing Engine Status

Action To display a detailed status of the Routing Engine, use the following JUNOS CLI operational mode command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status
 Slot 0
  Current state: Master
  Election priority: Master
 Temperature              41 C / 105 degrees F
  DRAM                     765 Mbytes
  CPU utilization
    User                     0 percent
    Background               0 percent
    Kernel                   0 percent
    Interrupt               0 percent
    Idle                   100 percent
  Serial ID                   39000004f8bdec01
  Start time                   2000-01-04 22:02:58 UTC
  Uptime                       14 hours, 45 minutes, 40 seconds
  Load averages                1 minute   5 minute  15 minute
                                    0.05       0.04       0.01
 Slot 1
  Current state   Backup
  Election priority   Backup (default)
  Temperature               41 C / 105 degrees F
  DRAM                     765 Mbytes
  CPU utilization
    User                     0 percent
    Background               0 percent
    Kernel                    0 percent
    Interrupt                2 percent
    Idle                    98 percent
  Serial ID                     f2000004f903a801
  Start time                     2000-01-04 01:28:02 UTC
  Uptime                         20 hours, 38 minutes, 1 seconds
```

What It Means The command output displays the Routing Engine slot number, current state (Master, Backup, or Disabled), election priority (Master or Backup), and the airflow temperature. The command output also displays the total DRAM available to the Routing Engine processor, the CPU utilization percentage, and the Routing Engine serial number for the slot. The command output displays when the Routing Engine started running, how long the Routing Engine has been running, and the time, uptime, and load averages for the last 1, 5, and 15 minutes.

Check the Uptime to ensure that the Routing Engine has not rebooted since it started running.

Alternative Actions

(For M7i, M10i, M40e, M160, M320, and T320 routers and the T640 routing node) To check the status and temperature of the Routing Engines, use the following CLI command:

user@host> **show chassis environment routing-engine**

```
user@host> show chassis environment routing-engine
Route engine 0 status:
  State:                      Present Master
  Temperature:              0 degrees C / 32 degrees F
Route engine 1 status:
  State:                      Present
```

The command output displays the Routing Engine slot number, operating state, temperature, and whether it is operating as the master or backup. The state can be Present or Absent.

To check the status and temperature of a particular Routing Engine, use the following CLI command:

user@host> **show chassis environment routing-engine** *slot*

Step 2: Check the Routing Engine LEDs

Steps To Take

To check the Routing Engine status LEDs, do one of the following:

1. Check the M7i Routing Engine LEDs on page 139
2. Check the M10i Router Routing Engine LEDs on page 139
3. Check the M20 Router Routing Engine LEDs on page 140
4. Check the M40 Router Routing Engine LEDs on page 142
5. Check the M40e and M160 Router Routing Engine LEDs on page 143
6. Check the M320 Router Routing Engine LEDs on page 144
7. Check the T320 Router Routing Engine LEDs on page 144
8. Check the T640 Routing Node Routing Engine LEDs on page 145

Check the M7i Routing Engine LEDs

Action Check the four LEDs located on the Routing Engine faceplate. A green LED labeled HDD, a blue LED labeled MASTER, a red LED labeled FAIL, and a green LED labeled ONLINE indicate Routing Engine status. Table 34 describes the LED states.

Table 34: M7i and M10i Router Routing Engine LED States

Label	Color	State	Description
HDD	Green	Blinking	There is read/write activity on the PC card.
MASTER	Blue	On steadily	Routing Engine is functioning as master.
FAIL	Red	On steadily	Routing Engine is not operational.
ONLINE	Green	On steadily	Routing Engine is running normally.

Check the M10i Router Routing Engine LEDs

The M10i router Routing Engine has four LEDs indicating Routing Engine status: a green LED labeled HDD, a blue LED labeled MASTER, a red LED labeled FAIL, and a green LED labeled ONLINE.

Figure 44: M10i Routing Engine LEDs

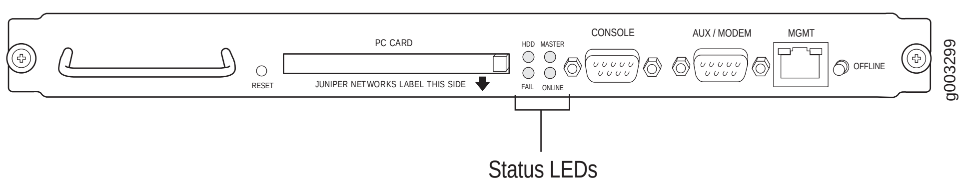


Table 35 describes the M10i router Routing Engine LEDs.

Table 35: M10i Router Routing Engine LEDs and Buttons

Label	Color	State	Description
HDD	Green	Blinking	There is read/write activity on the PC card.
MASTER	Blue	On steadily	Routing Engine is functioning as master.
FAIL	Red	On steadily	Routing Engine is not operational.
OFFLINE	Green	On steadily	Routing Engine is running normally.

You can see the Routing Engine LEDs on the Routing Engine panel located on the back of the router.

Check the M20 Router Routing Engine LEDs

The M20 router Routing Engine LEDs and buttons are located near the middle of the craft interface above and below the Juniper Networks logo (see Figure 45).

Figure 45: M20 Router Craft Interface Routing Engine LEDs and Buttons

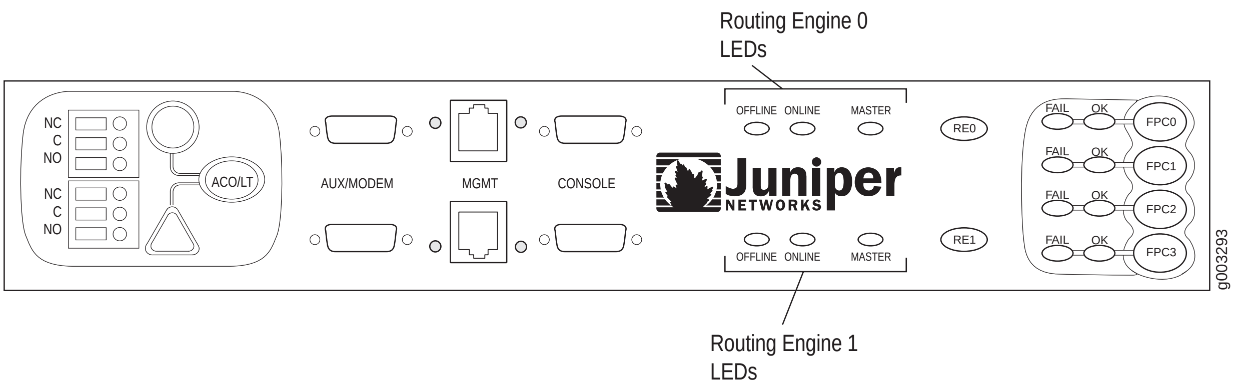


Table 36 describes the M20 router Routing Engine LEDs.

Table 36: M20 Router Routing Engine LEDs and Buttons

Label	Shape	Color	State	Description
MASTER	□	Blue	On steadily	Routing Engine is functioning as master.
ONLINE	□	Green	On steadily	Routing Engine has successfully booted and is running normally.
OFFLINE	○	Amber	On steadily	Routing Engine is not operational, or is in reset mode.
RE0, RE1	⬭	—	—	Press to take the Routing Engine offline.

You can see the Routing Engine LEDs on the craft interface or on the Routing Engine panel located on the back of the router (see Figure 46).

Figure 46: M20 Router Routing Engine Panel

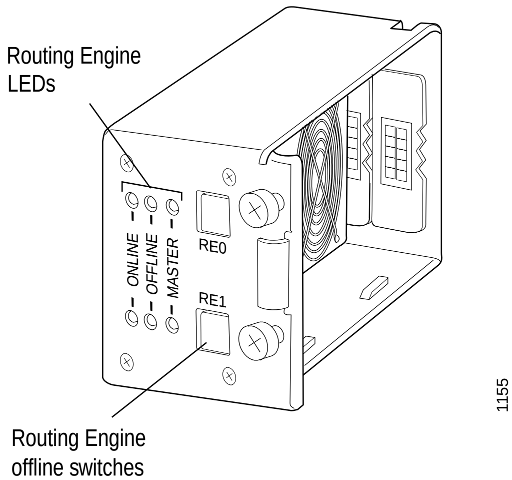


Figure 37 describes the Routing Engine panel LEDs.

Table 37: Routing Engine Panel LEDs

Label	Color	State	Description
OFFLINE	Amber	On steadily	Routing Engine is not operational or is in reset mode.
ONLINE	Green	On steadily	Routing Engine is running normally.
MASTER	Blue	On steadily	Routing Engine is functioning as master.

Check the M40 Router Routing Engine LEDs

Check the Routing Engine LEDs on the bottom right of the craft interface. A red Fail LED and a green OK LED indicate the status of the Routing Engine. The green OK LED should light steadily. Figure 47 shows the Routing Engine LEDs.

Figure 47: M40 Router Craft Interface Routing Engine LEDs

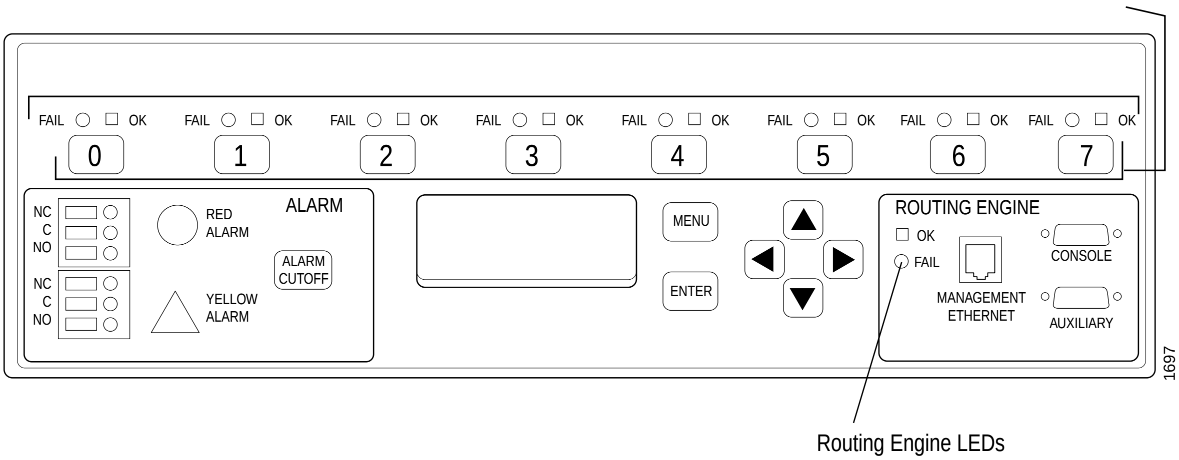


Table 38 describes the Routing Engine LED states.

Table 38: M40 Router Routing Engine LEDs

Label	Shape	Color	State	Description
OK	□	Green	On steadily	Presence of the Routing Engine is detected by the System Control Board (SCB).
OK	□	Green	Blinking	Routing Engine is starting up.
FAIL	○	Red	On steadily	Presence of the Routing Engine is not detected by the SCB, or the Routing Engine is not operational.

Check the M40e and M160 Router Routing Engine LEDs

Check the host module LEDs on the upper right of the craft interface. Three LEDs—one green MASTER, one green ONLINE, and one red OFFLINE—indicate the status of each host module. The LEDs marked HOST0 show the status of the Routing Engine in slot RE0 and the MCS in slot MCS0. The LEDs marked HOST1 show the status of the Routing Engine in slot RE1 and the MCS in slot MCS1.

Figure 48 shows the host module LEDs on the M40e and M160 router craft interface.

Figure 48: M40e and M160 Router Redundant Host Module LEDs

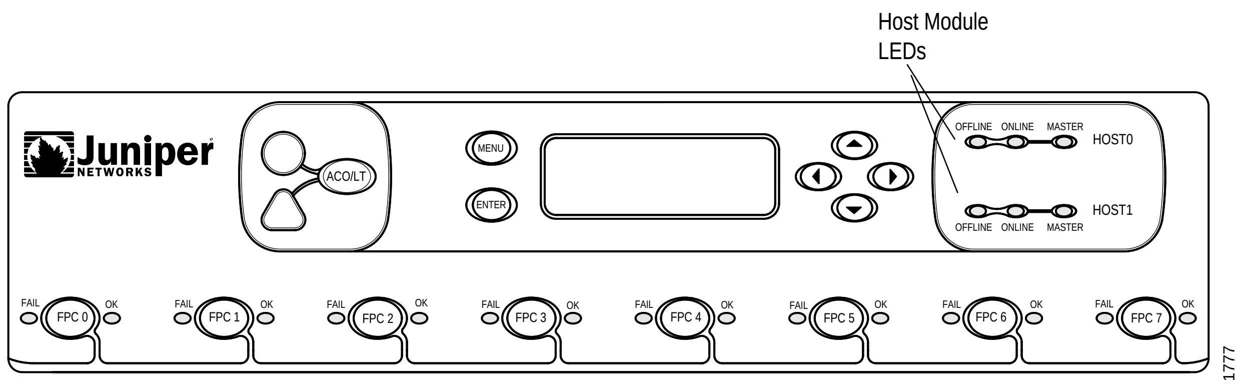


Table 39 describes the host module LEDs.

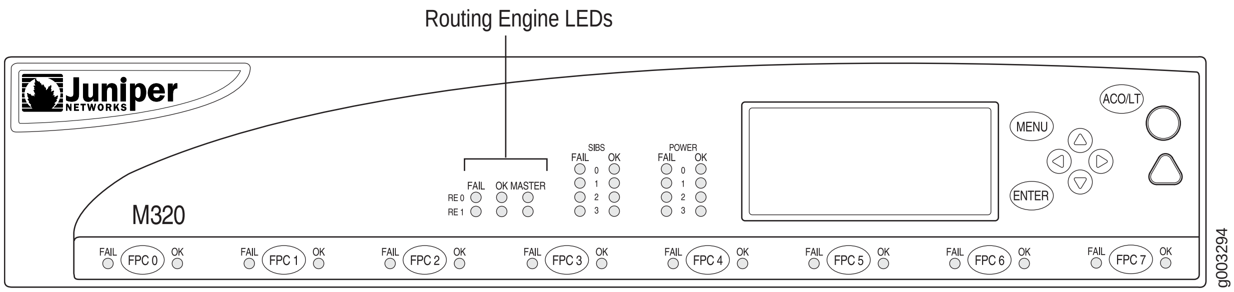
Table 39: M40e and M160 Router Host Module LEDs

Label	Shape	Color	State	Description
MASTER	◯	Green	On steadily	Host module (Routing Engine and MCS) is functioning as master.
ONLINE	◯	Green	On steadily	Host module is present and operational.
			Blinking	Host module is starting up.
OFFLINE	◯	Red	On steadily	Host module is not present, or is present but not operational.

Check the M320 Router Routing Engine LEDs

Figure 49 shows the host module LEDs on the M320 router craft interface.

Figure 49: M320 Router Redundant Host Module LEDs



Each host subsystem has three LEDs, located in the middle of the craft interface, that indicate status. The LEDs labeled RE0 show the status of the Routing Engine in slot RE0 and the Control Board in slot CB0. The LEDs labeled RE1 show the status of the Routing Engine in slot RE1 and the Control Board in slot CB1. Table 40 describes the functions of the host subsystem LEDs.

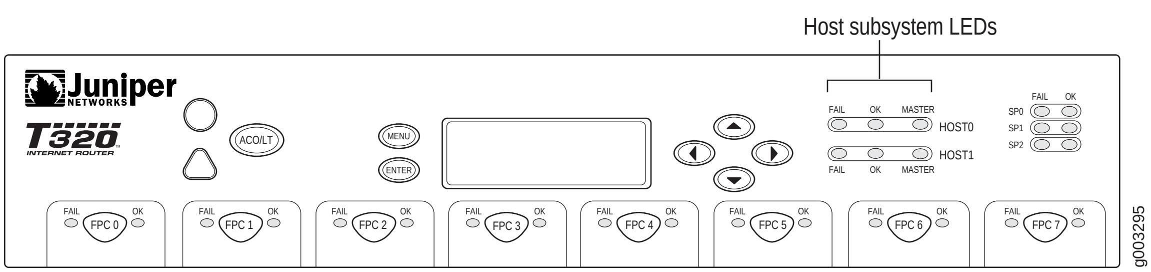
Table 40: M320 Router Host Subsystem LEDs

Label	Color	State	Description
FAIL	Red	On steadily	Host module is offline.
OK	Green	On steadily	Host module is online and functioning normally.
MASTER	Green	On steadily	Host module is functioning as master.

Check the T320 Router Routing Engine LEDs

Figure 50 shows the host module LEDs on the T320 router craft interface.

Figure 50: T320 Router Redundant Host Module LEDs



Each host subsystem has three LEDs, located on the upper right of the craft interface, which indicate status. The LEDs labeled HOST0 show the status of the Routing Engine in slot RE0 and the Control Board in slot CB0. The LEDs labeled HOST1 show the status of the Routing Engine in slot RE1 and the Control Board in slot CB1.

Table 41 describes the functions of the host subsystem LEDs.

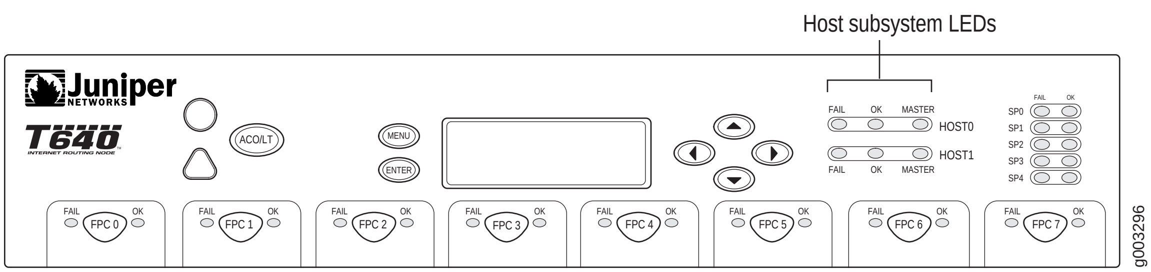
Table 41: T320 Router Host Subsystem LEDs

Label	Color	State	Description
OK	Green	On steadily	Host module is online and functioning normally.
FAIL	Red	On steadily	Host module is offline.
MASTER	Green	On steadily	Host module is functioning as master.

Check the T640 Routing Node Routing Engine LEDs

Figure 51 shows the host module LEDs on the T640 routing node craft interface.

Figure 51: T640 Routing Node Redundant Host Module LEDs



Each host subsystem has three LEDs, located on the upper right of the craft interface, which indicate status. The LEDs labeled HOST0 show the status of the Routing Engine in slot RE0 and the Control Board in slot CB0. The LEDs labeled HOST1 show the status of the Routing Engine in slot RE1 and the Control Board in slot CB1. Table 42 describes the functions of the host subsystem LEDs.

Table 42: T640 Routing Node Host Subsystem LEDs

Label	Color	State	Description
OK	Green	On steadily	Host module is online and functioning normally.
FAIL	Red	On steadily	Host module is offline.
MASTER	Green	On steadily	Host module is functioning as master.

Step 3: Check the Redundant Routing Engine Status from the Craft Interface CLI Output

Action To view the Routing Engine status from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
```

For M10i routers:

```
Red alarm:               LED off, relay off
Yellow alarm:            LED on, relay on
Routing Engine OK LED:   On
Routing Engine fail LED: Off

FPCs     0  1
-------------
Green    *  *
Red      .  .

LCD screen:
      +--------------------+
      |waddle              |
      |1 Alarm active      |
      |Y: Backup RE Active |
      |                    |
      +--------------------+
```

For M20 routers:

```
Red alarm:               LED off, relay off
Yellow alarm:            LED off, relay off
Routing Engine OK LED:   On
Routing Engine fail LED: Off

FPCs     0  1  2  3
-------------------
Green    .  *  *  .
Red      .  .  .  .

LCD screen:
     +--------------------+
     |myrouter            |
     |Up: 5+00:16:57      |
     |                    |
     |0pps Load           |
     +--------------------+
```

For M40e/M160 routers:

```
FPM Display contents:
    +--------------------+
    |myrouter            |
    |1 Alarm active      |
    |Y: PEM 0 Absent     |
    |                    |
    +--------------------|
```

```
Front Panel System LEDs:
Host     0    1
------------------------
OK       *    *
Fail     .    .
Master   *    .
```

For M320 routers:

```
FPM Display contents:
[...Output truncated...}
Front Panel System LEDs:
Routing Engine    0    1
--------------------------
OK                *    .
Fail              .    .
Master            *    .


[...Output truncated...]
```

For T320 routers:

```
FPM Display contents:
[...Output truncated...}
Front Panel System LEDs:
Routing Engine    0    1
--------------------------
OK                *    .
Fail              .    .
Master            *    .
[...Output truncated...]
```

For T640 routing nodes:

```
FPM Display contents:
     +--------------------+
     |bananas-re0         |
     |Up: 7+00:20         |
     |                    |
     |Fans OK             |
     +--------------------|

Front Panel System LEDs:
Routing Engine    0    1
--------------------------
OK                *    .
Fail              .    .
Master            *    .

Front Panel Alarm Indicators:
-----------------------------
Red LED      .
Yellow LED   .
Major relay  .
Minor relay  .
```

```
Front Panel FPC LEDs:
FPC    0   1   2   3   4   5   6   7
------------------------------------
Red    .   *   .   .   .   .   .   .
Green  *   .   *   *   .   *   .   .

CB LEDs:
    CB   0   1
--------------
Amber  .   .
Green  *   .
Blue   *   .

SCG LEDs:
   SCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

SIB LEDs:
   SIB  0   1   2   3   4
--------------------------
Red    .   .   .   .   .
Green  *   *   *   *   *
```

What It Means The M10i router craft interface command output displays the LED status of the master Routing Engine, indicating whether the OK and Fail LEDs are on or off. It also displays that the backup Routing Engine is active.

The M20 router craft interface command output displays the LED status of the master Routing Engine, indicating whether the OK and Fail LEDs are on or off.

The M40e and M160 router craft interface command output also displays the LED status of both the master and backup host modules that include the master and backup Routing Engines. By default, the master host module (Host 0) has components installed in slots RE0 and MCS0; the backup host module (Host 1) has components installed in slots RE1 and MCS1.

The T640 routing node craft interface command output indicates that RE0 is the master Routing Engine, and that it is active. The status under the backup Routing Engine (RE1) has no indicators.

Verifying Routing Engine Failure

NOTE: Routing Engine failures can include compact flash failure and hard disk failure. If the Routing Engine has a compact flash failure and hard disk failure at the same time, you will not be able to boot up the Routing Engine.

The following sections describe how to check for the following failure conditions:

NOTE: The M7i and M10i routers by default come with no compact flash.

Steps To Follow

1. Check Core Files If the Routing Engine Reboots on page 149
2. Example of Boot Messages If Routing Engine Fails to Boot on page 150
3. Check for Compact Flash Media and Hard Disk Failure on page 150

Step 1: Check Core Files If the Routing Engine Reboots

List the Core Files Generated After A Crash Occurs

A vmcore file is only generated if the Routing Engine has a kernel crash. Kernel crashes can be generated by such things as a bug in the kernel software or bad memory. If the router has a kernel crash, the vmcore.<*n*> file is generated while the Routing Engine comes back up.

Action A vmcore file is always saved in /var/crash/. To view the core file that is generated when a crash occurs, use the following CLI command:

user@host> **file list /var/crash/ detail**

Sample Output

```
user@host> file list /var/crash/ detail
/var/crash/:
total 892856
-rw-r--r--  1 root  wheel          2 May 14  2004 bounds
-rw-r--r--  1 root  wheel   11959693 Oct 13  2003 kernel.0
-rw-r--r--  1 root  wheel   10114127 May 14  2004 kernel.1
-rw-r--r--  1 root  wheel          5 Feb 26  1997 minfree
-rw-------  1 root  wheel  805240832 Oct 13  2003 vmcore.0
-rw-------  1 root  wheel  805240832 May 14  2004 vmcore.1
```

What It Means The command output lists the vmcore.<*n*> files that have been generated.

Display the Messages Log File After A Crash Occurs

Action You might see the following in the /var/log/messages file after the router comes back up after a kernel crash occurred. To view the messages log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Mar  9 12:22:02 host savecore: Router crashed.....
Mar  9 12:22:02 host savecore: reboot after panic: Loss of soft watchdog Mar  9
12:22:02 host savecore: system went down at Sun Mar  9 12:22:02 2003 Mar  9
12:22:02 host savecore: Selective dump will be saved now
```

What It Means A kernel crash occurred and a core file has been generated.

Example of When No Core File Is Generated

When a power outage occurs, no kernel crash core file is generated. To view the messages log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Aug 15 15:35:58 host /kernel: checking for core dump...
Aug 15 15:35:59 host /kernel: savecore: Router rebooted. Cause unknown....
Aug 15 15:35:59 host savecore: Router rebooted. Cause unknown....
```

What It Means The kernel checks for a core dump file when the router reboots.

Example of Boot Messages If Routing Engine Fails to Boot

The following example shows boot messages that occur when a Routing Engine remains in a constant boot loop. In this condition, contact JTAC for further analysis and assistance.

```
Trying to boot from PCMCIA Flash Card ...
Trying to boot from Compact Flash ...
Trying to boot from Ethernet ...
```

Step 2: Check for Compact Flash Media and Hard Disk Failure

If the Routing Engine has a compact flash failure, the router boots from the hard disk. When you log in to the router, the JUNOS software CLI will indicate that the router has booted from alternate media.

If the Routing Engine has a hard drive failure, the router boots from the compact flash as usual. However, the router cannot write to the hard drive.

When the Compact Flash Is Removed from the Boot List

You can have a compact flash error when conditions, such as a HARD READ error occurs. When the compact flash is removed from the boot list, the following message displays you log in to the router:

```
login: user

--- JUNOS 6.0R1.6 built 2003-09-24 04:06:27 UTC
---
--- NOTICE: System is running on alternate media device     (/dev/ad1s1a).
---

user@host>
```

Action Check to see which file system is mounted by using the following CLI command:

```
user@host> show system storage
```

Sample Output

```
user@host> show system storage
Filesystem       512-blocks       Used      Avail Capacity Mounted on
/dev/ad1s1a          218690      56502     144694      28%  /
devfs                    32         32          0     100%  /dev/
/dev/vn0              18316      18316          0     100%  /packages/mnt/jbase
devfs                    32         32          0     100%  /dev/
/dev/vn1              45448      45448          0     100%
/packages/mnt/jkernel-6.0R1.6
/dev/vn2              20532      20532          0     100%
/packages/mnt/jpfe-M160-6.0R1.6
/dev/vn3               3580       3580          0     100%
/packages/mnt/jdocs-6.0R1.6
/dev/vn4              20728      20728          0     100%
/packages/mnt/jroute-6.0R1.6
/dev/vn5               9256       9256          0     100%
/packages/mnt/jcrypto-6.0R1.6
mfs:139             4064278          2    3739134       0%  /tmp
/dev/ad1s1e           24234          4      22292       0%  /config
procfs                    8          8          0     100%  /proc
/dev/ad1s1f        52492630    7988510   40304710      17%  /var
```

What It Means The command output will not show ad0 (the compact-flash) mounted, but instead, ad1 (the hard disk) has the root file system mounted.

Determine Why Compact Flash Did Not Mount

Action To determine why the compact-flash did not get mounted, use the following CLI command:

```
user@host> show system boot-messages | match "ad0|ad1"
```

```
user@host> show system boot-messages | match "ad0|ad1"
ad0: not attached, missing in Boot List
ad1: 28615MB <FUJITSU MHS2030AT> [58140/16/63] at ata0-slave using BIOSDMA
Mounting root from ufs:/dev/ad1s1a
```

What It Means The command output shows that the compact flash (ad0) was removed from the boot list.

When the Hard Disk Is Removed from the Boot List

The following boot messages list on the console shows symptoms that signify a hard disk failure. These messages are not in the boot-messages log file.

Sample Output

```
/dev/ad1s1f: CAN'T CHECK FILE SYSTEM.
/dev/ad1s1f: UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.
Can't open /dev/ad1s1f: Device not configured
WARNING:
WARNING: /var mount failed, building emergency /var
WARNING:
dumpon: sysctl: kern.dumpdev: Device not configured
mgd: commit complete
dumpon: sysctl: kern.dumpdev: Device not configured
mgd: commit complete
```

What it Means The boot messages show that the hard disk (ad1) was removed from the boot list (using JUNOS, release 6.1R1.4).

Verify That the Hard Disk Did Not Mount

Action To verify that the hard disk (ad1) did not get mounted, use the following CLI command:

user@host> **show system storage**

Sample Output The following sample output was taken from a RE-333 Routing Engine.

```
user@host> show system storage
Filesystem       512-blocks      Used      Avail Capacity Mounted on
/dev/ad0s1a          218690     60294     140902     30%  /
devfs                    32        32          0    100%  /dev/
/dev/vn0              20044     20044          0    100%  /packages/mnt/jbase
devfs                    32        32          0    100%  /dev/
/dev/vn1              51920     51920          0    100%
/packages/mnt/jkernel-6.1R1.4
/dev/vn2              22328     22328          0    100%
/packages/mnt/jpfe-M160-6.1R1.4
/dev/vn3               3844      3844          0    100%
/packages/mnt/jdocs-6.1R1.4
/dev/vn4              23328     23328          0    100%
/packages/mnt/jroute-6.1R1.4
/dev/vn5               8820      8820          0    100%
/packages/mnt/jcrypto-6.1R1.4
mfs:139              127006     16914      99932     14%  /tmp
/dev/ad0s1e           24234        28      22268      0%  /config
procfs                    8         8          0    100%  /proc
```

What It Means The command shows that the hard disk (ad1) is not mounted. Instead, /var now exists only in the swap partition (mfs:139), so any contents saved to /var will not be saved at the next reboot.

```
user@host> start shell
user@host% ls -l /
total 47
-rw-r--r--  1 root  wheel  4735 Mar 31  2001 COPYRIGHT
dr-xr-xr-x  2 root  wheel   512 Jan 20  2004 altconfig
dr-xr-xr-x  2 root  wheel   512 Jan 20  2004 altroot
drwxr-xr-x  2 root  wheel   512 Dec 29 12:00 bin
```

```
dr-xr-xr-x  3 root  wheel   512 Feb  4 23:16 boot
drwxr-xr-x  3 root  wheel   512 Feb  3 18:08 config
dr-xr-xr-x  4 root  wheel  2084 Feb  4 23:18 dev dr-xr-xr-x  7 root  wheel  1536
Feb  4 23:19 etc
lrwxr-xr-x  1 root  wheel    17 Dec 29 12:02 kernel -> /packages/jkernel
dr-xr-xr-x  2 root  wheel   512 Jan 20  2004 mnt
drwxr-xr-x  2 root  wheel   512 Feb  3 21:16 modules
drwxr-xr-x  3 root  wheel  1536 Feb  3 21:19 packages
dr-xr-xr-x  1 root  wheel   512 Feb  4 23:29 proc
dr-xr-xr-x  2 root  wheel   512 Feb  3 21:15 root
dr-xr-xr-x  3 root  wheel  1536 Feb  3 21:15 sbin
drwxrwxrwt  3 root  wheel   512 Feb  4 23:19 tmp
dr-xr-xr-x  8 root  wheel   512 Dec 29 12:00 usr
lrwxr-xr-x  1 root  wheel     8 Feb  4 23:18 var -> /tmp/var
```

What It Means The example shows that var has a symbolic link to the /tmp/var directory. It resides under the /tmp/var directory, and is mounted on the mfs partition.

Verify That the Hard Disk Is Missing from The Boot List

Action To verify that the hard disk (ad1) is missing from the boot list, use the following CLI command:

user@host> **show system boot-messages | match "ad0|ad1"**

Sample Output

```
user@host> show system boot-messages | match "ad0|ad1"
ad0: 122MB <SanDisk SDCFB-128> [980/8/32] at ata0-master using PIO4
ad1: not attached, missing in Boot List
Mounting root from ufs:/dev/ad0s1a
```

What It Means The device is taken out of the boot list because of an error condition, such as a HARD READ errror.

View Alarms When Media Is Removed from the Boot List

Action To display an alarm that is generated when media (compact flash or hard disk) is removed from the boot list, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2005-02-04 23:19:27 CET  Major  hard-disk missing in Boot List
```

What It Means When the router is operational and the hard disk is removed from the boot list, a minor yellow alarm is generated. When the router is rebooted and the hard disk is still removed from the boot list, a red major alarm is generated.

What It Means The command output displays a major alarm indicating what media is missing from the boot list and the time and date when the event occurred.

Step 3: Understand What Happens When Memory Failures Occur

Most Juniper Networks Routing Engines support Error Checking and Correction (ECC) protected memory. There are two types of memory errors: single-bit and multiple-bit.

A single-bit error is when a single 0 or 1 bit is incorrect. The system detects and corrects single-bit errors, then logs the event in the /var/log/eccd file. If there are persistent single-bit errors, the Routing Engine controller reboots the Routing Engine. Persistent single-bit errors could be a symptom of bad RAM.

Multiple-bit errors are when multiple bits are incorrect. By default, if a multiple-bit error is detected, a nonmaskable interrupt (NMI) is generated to interrupt the Routing Engine and panic the kernel causing the router to subsequently reboot. The Routing Engine panics the kernel, and leaves a vmcore file.Multi-bit parity error detection was implemented in JUNOS software release 5.3 and above.

Step 4: Check the Router File System and Boot Disk

Action Table 43 specifies the storage media by Routing Engine type. The device names are displayed when the router boots. To display the Routing Engine type on some routers, use the show chassis hardware CLI command.

Table 43: Storage Media Device Names

Storage Media	RE-M40 (RE1)	RE-400 (RE5)	RE-333 (RE2)/ RE-600 (RE3)	RE-1600 (RE4)
Flash drive	ad0	ad0	ad0	ad0
Hard disk	ad2	ad1	ad1	ad1
Removable media	afd0	ad3	ad3	ad3 and ad4

Action To check the router file system and on which disk the router booted, use the following CLI command:

user@host> **show system storage**

Sample Output

```
user@host> show system storage
  Filesystem  1K-blocks     Used    Avail Capacity  Mounted on
  /dev/ad0s1a     65687    26701    33732    44%    /
  devfs              16       16        0   100%    /dev/
  /dev/vn1         9310     9310        0   100%    /packages/mnt/jbase
  /dev/vn2         8442     8442        0   100%
/packages/mnt/jkernel-5.0R5.1
  /dev/vn3        11486    11486        0   100%    /packages/mnt/jpfe-5.0R5.1
  /dev/vn4         5742     5742        0   100%    /packages/mnt/jroute-5.0R5.1
  /dev/vn5         1488     1488        0   100%
/packages/mnt/jcrypto-5.0R5.1
  /dev/vn6          792      792        0   100%    /packages/mnt/jdocs-5.0R5.1
  mfs:181        762223        3   701243     0%    /tmp
  /dev/ad0s1e     25263        7    23235     0%    /config
  procfs              4        4        0   100%    /proc
  /dev/ad1s1f   7156052   337194  6246374     5%    /var
```

What It Means The command output displays statistics about the amount of free disk space in the router's file systems, including the amount used, the amount available, and the percentage of system space being used. The values are displayed in 1024-byte (1KB) blocks.

Filesystem is the name of the file system on which the Routing Engine booted. The command output also displays the directory to which the file system is mounted. During normal operation, the / and /config directories are from the compact flash drive and the /var directory is from the hard drive. If the router booted off the hard drive, the show system storage command will show all three directories on the hard drive. If the hard drive fails and the router booted off the compact flash drive, the show system storage command will show all three directories on the compact flash drive.

Step 5: Display the Current Routing Engine Alarms

To display information about the conditions that trigger Routing Engine alarms for each router type, see "Display the Current Router Alarms" on page 61.

NOTE: An event may occasionally cause the Routing Engine not to boot and you will not be able to display the current alarms.

Action To display the current Routing Engine alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2001-07-22 15:12:19 PDT  Major  hard-disk missing in Boot List
2002-05-14 09:20:36 PDT  Major  compact-flash missing in Boot List
2002-05-14 09:20:31 PDT  Minor  Boot from alternate media
```

What It Means The command output displays the alarm time, severity level, and description.

Step 6: Display Error Messages in the System Log File

Action To view Routing Engine error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output For compact flash drive errors:

```
user@host> show log messages
Feb  3 07:58:17 host /kernel: ad0: HARD WRITE ERROR blk# 135783 status=51
error=10 Feb  3 07:58:17 host /kernel: ad0: HARD WRITE ERROR blk# 137633
status=51 error=10 Feb  3 07:58:47 host /kernel: ad0: HARD WRITE ERROR blk#
135731 status=51 error=10 Feb  3 07:58:47 host /kernel: ad0: HARD WRITE ERROR
blk# 135783 status=51 error=10 Feb  3 07:58:47 host /kernel: ad0: HARD WRITE
ERROR blk# 137633 status=51 error=10
```

For hard drive errors:

```
user@host> show log messages
Jun  3 12:00:28 router /kernel: ad1: WRITE command timeout - resetting
Jun  3 12:00:44 router /kernel: ata0: resetting devices ..
Jun  3 12:00:44 router /kernel: ata0:  Succeeded in resetting devices.
Jun  3 12:00:28 router /kernel: ad1: WRITE command timeout - resetting
Jun  3 12:00:17 router /kernel: ata0: resetting devices ..
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Use the show log messages CLI command to browse error messages that are generated at least 5 minutes before and after an event. You can also use the show log messages | match "*device-name*" command to view error messages that are specific to a device name. Use this information to diagnose a problem and to let JTAC know what error messages were generated and the router events prior to the event. For more information about system log messages, see the *JUNOS Software System Log Messages Reference*.

Step 7: Document the Events Prior to the Failure

Action To document events that occurred prior to a Routing Engine failure, follow these steps:

1. Write down any events such as an abrupt router shutdown because of a power outage, a software upgrade, a configuration commit, or a system snapshot request.

2. Write down any recovery procedures attempted. If the Routing Engine reported some errors on the hard drive but appeared to be working fine or a backup Routing Engine is available, it may not be necessary to recover.

3. Turn on logging to your console to start capturing screen output. This is especially useful if a terminal server is connected to the Routing Engine console port.

4. While you have screen capturing enabled, boot the Routing Engine and look at the router boot messages.

Getting Routing Engine Hardware Information

Steps To Take To get hardware information for a failed Routing Engine, follow these steps:

1. Display Routing Engine Hardware Information on page 157
2. Locate the Routing Engine Serial Number ID Label on page 158

Step 1: Display Routing Engine Hardware Information

Action To display the Routing Engine hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output For an M20 router with two Routing Engines:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis
Backplane        REV 03   710-001517   AA7915
Power Supply A   Rev 01   740-001465   000011            AC
Power Supply B   Rev 01   740-001465   000016            AC
Display          REV 04   710-001519   AE6019
Routing Engine 0                       32000004f8ff1201  RE-2.0
Routing Engine 1 REV 01   740-003239   AARCHOO           RE-2.0
[...Output truncated...]
```

For M40 router components:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Backplane        REV 02   710-000073   S/N AA0053
Power supply A   Rev 2    740-000235   S/N 000042        DC
Maxicab          REV X1   710-000229   S/N AA0139
Minicab          REV X1   710-000482   S/N AA0201
[...Output truncated...]
```

What It Means The sample output for an M20 router displays the Routing Engine, slot number, and serial number, and indicates that it is present in the router. Give this information to JTAC if the Routing Engine fails.

The sample output for an M40 router shows that the maxicab is the (Motorola) Routing Engine, and the minicab is the Routing Engine and Packet Forwarding Engine interface.

On other routers, the Routing Engine serial number is located in the host hardware inventory line.

Step 2: Locate the Routing Engine Serial Number ID Label

If the Routing Engine fails, you cannot see the Routing Engine hardware information when you use the show chassis hardware command. You must manually locate the serial number ID label on the component

Some Routing Engines may have more than one serial number. Contact your Juniper Networks support representative if you need assistance in determining which serial number to provide.

Action Look on the Routing Engine for the serial number ID label.

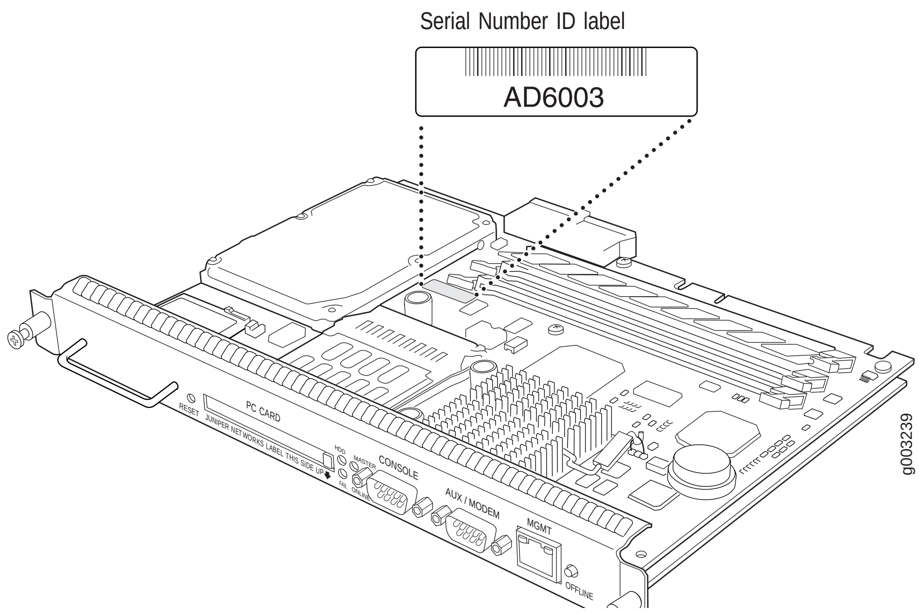
M7i Router Routing Engine Serial Number ID Label Location

The serial number ID label is located on the left side near the midplane connector.

M10i Router Routing Engine Serial Number ID Label Location

The serial number ID label is located on the left side, near the back (see Figure 52).

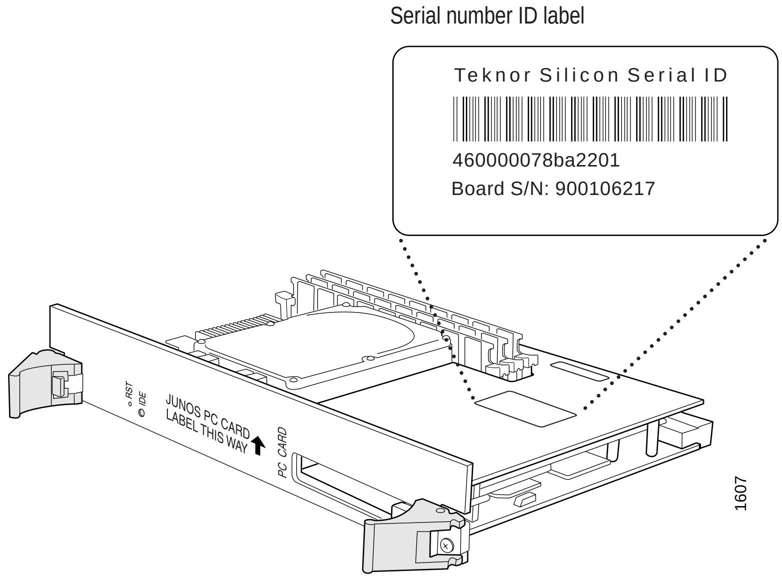
Figure 52: M10i Router Routing Engine Serial Number ID Label Location



Teknor Type 2 Routing Engine Serial Number ID Label Location

For all routers with a Type 2 (Teknor) Routing Engine, the serial number ID label is located on the top right side of the Routing Engine (see Figure 53 on page 159). If there are multiple labels on the Routing Engine, the label marked “Teknor Silicon Serial ID” is the correct serial number. The serial number ID label includes two serial numbers: a 16-digit number on the top and a 10-digit number on the bottom. Give both serial numbers to JTAC.

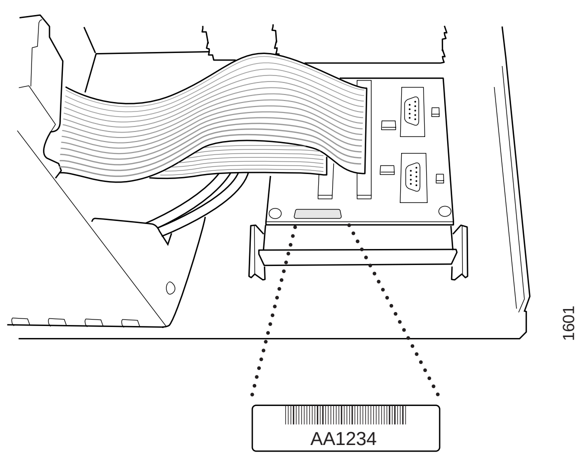
Figure 53: Routing Engine Serial Number ID Label Location for All Routers



M40 Router Routing Engine Serial Number ID Label Location

For M40 routers, the serial number that you use depends on whether you purchased the Routing Engine housing or just the Routing Engine. If you purchased the Routing Engine housing, the serial number is located on the maxicab, as shown in Figure 54. If you purchased the Routing Engine only, remove the Routing Engine and locate the serial number ID label, as shown in Figure 54. If there are multiple labels on the Routing Engine, the label marked “Teknor Silicon Serial ID” is the correct serial number.

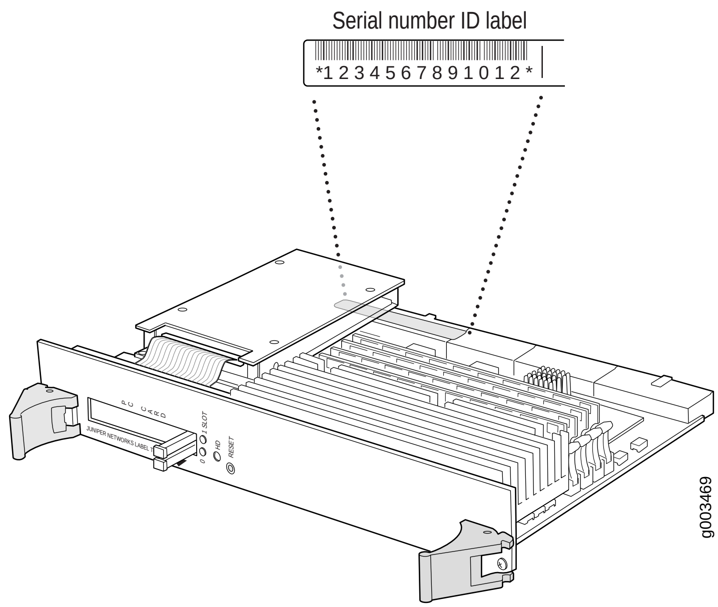
Figure 54: M40 Router Routing Engine Serial Number ID Label



M320 Router Serial Number ID Label Location

The serial number label is located on the right side of the top of the Routing Engine (see Figure 55).

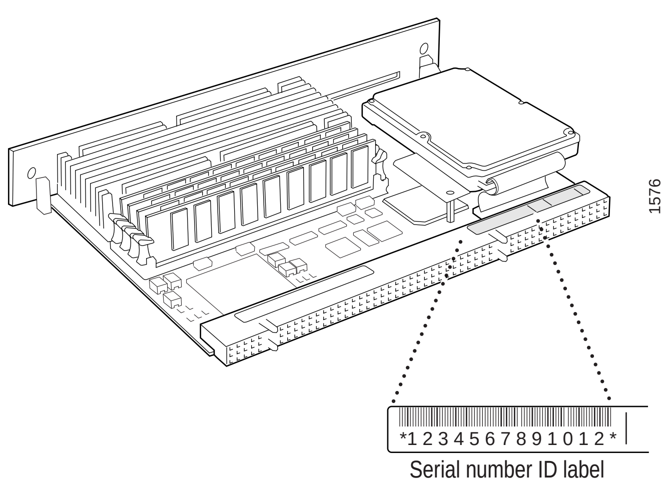
Figure 55: M320 Router Routing Engine Serial Number ID Label Location



T320 Router and T640 Routing Node Serial Number ID Label Location

For the T320 router and T640 routing node, the serial number ID label is located on the right side of the top of the Routing Engine (see Figure 56).

Figure 56: T320 Router and T640 Routing Node Routing Engine Serial Number ID Label



Removing a Routing Engine

Action To replace the Routing Engine, see the appropriate router hardware guide See also, “Replacing a Redundant Routing Engine” on page 506..

NOTE: The M5 and M10 routers have a cover over the Routing Engine. The M40e and M160 routers have a cover over all the rear chassis components.

Chapter 15

Monitoring FPCs

You monitor and maintain Flexible PIC Concentrators (FPCs) to connect Physical Interface Cards (PICs) to the rest of the router so that incoming packets are forwarded across the midplane to the appropriate destination ports. (See Table 44.)

Table 44: Checklist for Monitoring FPCs

Monitor FPC Tasks	Command or Action
Understanding FPCs on page 164	
■ FPC Numbering on page 165	
Checking the FPC Status on page 166	
1. Check FPC Status and Utilization on page 166	show chassis fpc
2. Check FPC Status and Uptime on page 167	show chassis fpc detail *fpc-slot*
3. (M40e, M160, M320, and T320 routers and T640 routing node only) Check FPC Status and Temperature on page 167	show chassis environment fpc *fpc-slot*
4. Check the FPC LED States on page 168	show chassis craft-interface Or, physically check the FPC LEDs on the Front Panel Module (FPM).
Checking for FPC Alarms on page 169	
1. Display the Current FPC Alarms on page 169	show chassis alarms
2. Display FPC Error Messages in the System Log File on page 170	show log messages | match “fpc| kernel | tnp”
3. Display FPC Error Messages in the Chassis Daemon Log File on page 171	show log chassisd | match fpc
Verifying FPC Failure on page 173	
1. Document Events Prior to the FPC Failure on page 173	Document a software upgrade, hardware upgrade, or reset.
2. Check the FPC Installation on page 173	Check that the FPC is seated in the slot. Try to bring the FPC online.
3. Check the FPC Fuses on page 174	The fuses for the and FPCs are located in the rear of the midplane behind the power supply in slot PEM0.
4. Take the FPC Offline on page 175	Press the offline button for approximately 3 seconds.
5. Perform an FPC Swap Test on page 176	Replace the FPC with one that you know works.
6. Display the FPC Software Version Information on page 176	show version brief
7. Display the FPC Hardware Information on page 177	show chassis hardware

Monitor FPC Tasks	Command or Action
8. Locate the FPC Serial Number ID Label on page 177	■ M20 Internet router—With the FPC in horizontal position, look on the top back right of the FPC. ■ M40 Internet router—With the FPC in vertical position, look on the back left side of the FPC. ■ M40e and M160 routers—With the FPC in vertical position, look on the center right side of the FPC. ■ For M320 routers—On an FPC3, the serial number ID label is located on the center of the right side. On an FPC2, the serial number label is located on the top PIC slot. ■ For T320 routers—On an FPC3, the serial number ID label is located on the center of the right side. On an FPC1 and FPC2, the serial number ID label is located near the top PIC slot. ■ For T640 routing nodes—On an FPC3, the serial number label is located on the center of the right side. On an FPC2, the serial number label is located near the top PIC slot.
Replacing an FPC on page 181	See "Return the Failed Component" on page 86. Follow the procedure in the appropriate router hardware guide.

Understanding FPCs

Purpose Inspect the FPCs to ensure that they connect PICs to the rest of the router so that incoming packets are forwarded across the midplane to the appropriate destination port.

What Is an FPC The FPC is a component of the Packet Forwarding Engine. FPCs house the various PICs used in the router.

The FPCs installed in the router depend on the platform and the PICs needed. Table 45 provides some FPC characteristics for each router type.

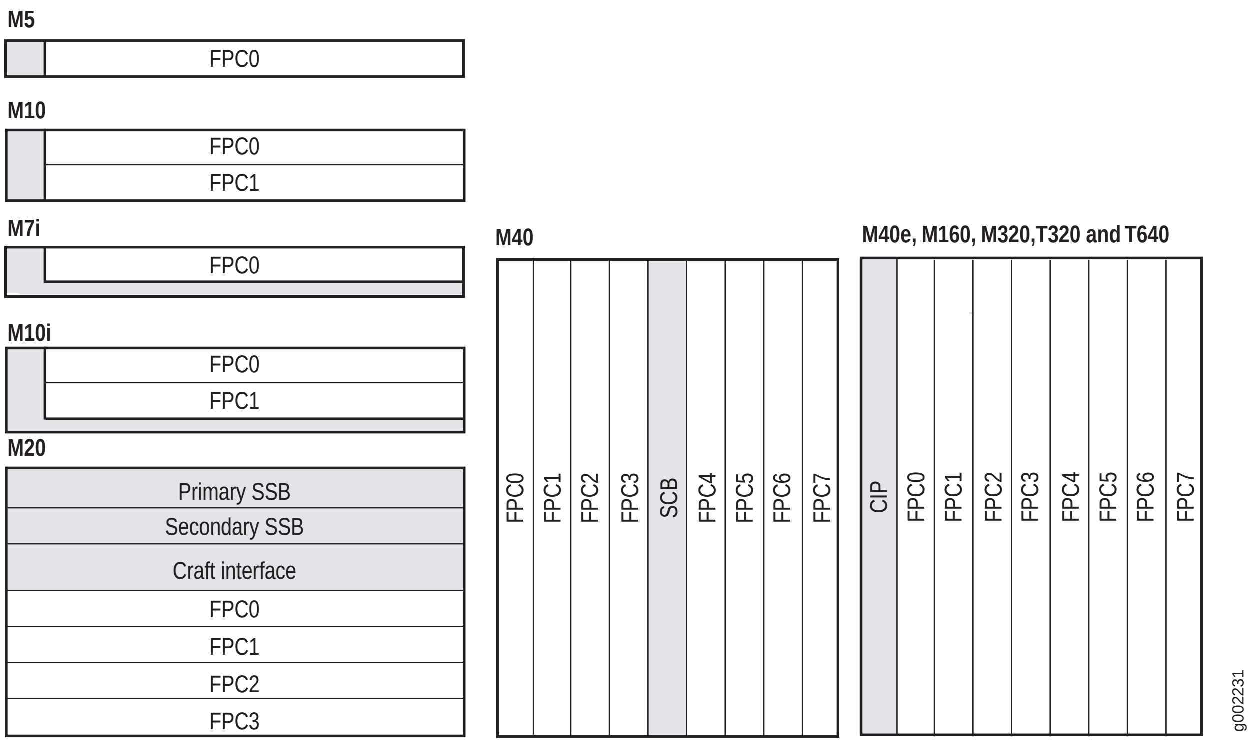
For a listing of available FPCs and supported PICs, see the appropriate router hardware guide and router PIC guide.

Table 45: FPC Characteristics Per Routing Platform

FPC Characteristic	M5/ M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
FPC types supported per router	FPC built into the FEB	FPC built into the router	FPC built into the router	FPC	FPC	M40e-FPC1, M40e-FPC2	FPC1, FPC2	FPC1, FPC2, FPC3	FPC1, FPC2, FPC3	FPC2, FPC3
FPC slots per router	1/2	1	2	4	8	8	8	8	8	8

Figure 57 shows the location and numbering of the FPCs in each router platform.

Figure 57: FPC Numbering



FPCs are hot-insertable and hot-removable. You can remove and replace them without powering down the router or disrupting the routing functions.

See Also "Monitoring PICs" on page 183

Checking the FPC Status

Steps To Take

To check the FPC status, follow these steps:

1. Check FPC Status and Utilization on page 166
2. Check FPC Status and Uptime on page 167
3. Check FPC Status and Temperature on page 167
4. Check the FPC LED States on page 168

Step 1: Check FPC Status and Utilization

Action

To display brief status and utilization information for all FPCs installed in the router, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis fpc**

Sample Output

```
user@m160> show chassis fpc
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           43      3          0        32          1         39
  1  Online           47      3          0        32          1         39
  2  Online           42      3          0        32          1         40
  3  Online           40      4          0        32          1         39
  4  Online           41      4          0        32          1         39
  5  Online           42      0          0        32          1         39
  6  Empty             0      0          0         0          0          0
  7  Empty             0      0          0         0          0          0
```

What It Means

Use the show chassis fpc command to identify whether there is a problem with any of the FPCs installed in the router. The command output displays a brief status of all the FPCs installed in the router. The state can be online, dead, diag, dormant, empty, online, probed, or probe-wait. If the FPC state is dead, an alarm occurs. For more detailed information about the FPC states, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference.*

The temperature is that of the air flowing past the FPC. If the temperature is too high, an alarm occurs.

The CPU and memory information is the total percentage of CPU being used by the FPC processor, the total CPU being used by the FPC processor, the percentage of CPU being used for interrupts, and the total DRAM available to the FPC processor. The percentage of heap space (dynamic memory) reflects the buffer space being used by the FPC processor. If the heap space exceeds 80 percent, there might be a software problem (memory leak).

The output also displays the percentage of buffer space being used by the FPC processor for buffering internal messages.

Step 2: Check FPC Status and Uptime

Action To display the status and uptime for a particular FPC slot, use the following CLI command:

user@host> **show chassis fpc detail** *fpc-slot*

Sample Output

```
user@M160> show chassis fpc detail 3
Slot 3 information:
  State                              Online
  Temperature                     36 degrees C / 96 degrees F
  Total CPU DRAM                  32 Mbytes
  Total SRAM                       4 Mbytes
  Total SDRAM                    256 Mbytes
  I/O Manager ASIC information       Version 2.0, Foundry IBM, Part number 0
  I/O Manager ASIC information       Version 2.0, Foundry IBM, Part number 0
  I/O Manager ASIC information       Version 2.0, Foundry IBM, Part number 0
  Start time:                        2002-03-19 13:13:26 PST
  Uptime:                            6 days, 1 hour, 19 minutes, 36 seconds
```

What It Means The command output shows status information for the FPC in slot 3, including the operating state. The state can be online, dead, diag, dormant, empty, online, probed, or probe-wait. If the FPC state is dead, an alarm occurs. For more detailed information about the FPC states, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference.* The command output also shows temperature, memory usage, I/O Manager application-specific integrated circuit (ASIC) version level, start time, and uptime. The uptime is important to determine how long the FPC has been operational. A small uptime means that the FPC came online a short time ago and could indicate a possible FPC error condition.

Syntax show chassis fpc <pic-status <*fpc-slot*>>
show chassis fpc <detail <*fpc-slot*>>

Step 3: Check FPC Status and Temperature

Action (M40e, M160, M320, and T320 routers and T640 routing node only) To display the FPC status and temperature for a particular FPC slot, use the following CLI command:

user@host> **show chassis environment fpc** *fpc-slot*

```
user@m160> show chassis environment fpc 0
FPC 0 status:
  State                          Online
  Temperature                 39 degrees C / 102 degrees F
  Power:
    1.5 V                   1496 mV
    2.5 V                   2485 mV
    3.3 V                   3306 mV
    5.0 V                   4991 mV
    5.0 V bias              4993 mV
    8.0 V bias              8251 mV
  CMB Revision                12
```

What It Means The command output displays the status of the FPC in slot 0, including the state, temperature, voltage levels on the FPC, and the revision level of the chassis management bus slave. The state can be Unknown, Empty, Present, Ready, Announce online, Online, Offline, or Diagnostics. An Offline state indicates an FPC error condition.

Step 4: Check the FPC LED States

Action To check the FPC LED status, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
Front Panel FPC LEDs:
FPC    0   1   2   3   4   5   6   7
-----------------------------------
Red    .   .   .   .   .   .   .   .
Green  *   *   .   .   .   .   .   .
[...Output truncated...]
```

What It Means The Front Panel FPC LEDs section displays the status of each FPC. The FPCs have two operational states: Green (OK), and Red (Fail). Asterisks (*) indicate the operating state. Dots indicate an off state for LEDs. If both red and green LEDs have dots, the FPC slot is empty. Asterisks in the Green state indicate that the FPCs in slots 0 and 1 are operating normally. No FPCs are installed in slots 2 through 7.

Alternative Action (For all routers except the M5, M7i, M10, and M10i) You can also check the FPC status by looking at the LEDs on the faceplate. Each FPC has two LEDs that report its status. Only one LED state can occur at a time. Table 46 describes the FPC LEDs.

Table 46: FPC LEDs on the Faceplate

Label	Shape	Color	State	Description
OK	□	Green	On steadily	FPC is functioning normally.
			Blinking	FPC is starting up.
FAIL	○	Red	On steadily	FPC has failed.

(For all routers except the M5, M7i, M10, and M10i, you can check the FPC status by looking at the FPC LEDs on the craft interface. Table 47 describes the functions of the FPC LEDs.

Table 47: FPC LEDs on the Craft Interface

Label	Color	State	Description
FAIL	Red	On steadily	FPC has failed.
OK	Green	On steadily	FPC is functioning normally.
		Blinking	FPC is starting up.

Checking for FPC Alarms

Steps To Take To check for FPC alarms, follow these steps:

1. Display the Current FPC Alarms on page 169
2. Display FPC Error Messages in the System Log File on page 170
3. Display FPC Error Messages in the Chassis Daemon Log File on page 171

Step 1: Display the Current FPC Alarms

Action You can display current FPC alarms at the command line or use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time              Class  Description
 2002-04-16 15:09:00 UTC Major  Too many unrecoverable errors
```

What It Means The command output displays the current FPC alarms, including the time the alarm occurred, the severity level, and the alarm description. At the command line, you see the following FPC error messages:

```
Too many unrecoverable errors
Too many recoverable errors
```

From the router craft interface LCD screen, you see the following:

```
Slot x: errors
```

Alternative Actions Check for FPC alarms on the router craft interface. You can physically look at the craft interface or use the show chassis craft-interface command. When a red or yellow alarm occurs, the craft interface goes into alarm mode. Alarm mode preempts idle mode, displaying a message to alert you of serious alarm conditions. In alarm mode, the screen displays the following information:

```
+--------------------+
|myrouter            |
|1 Alarm active      |
|R: Slot 2:errors    |
|                    |
+--------------------+
```

The craft interface output provides the following information:

- First line—Name of the router.
- Second line—Number of alarms active on the router.
- Third and fourth lines—Individual alarms, with the most severe condition shown first. Each line indicates whether the alarm is a red (R) or yellow (Y) alarm.

For more information about the craft interface, see “Monitoring the Craft Interface” on page 197 or the appropriate hardware guide.

For more information about craft interface alarms, see “Display the Current Router Alarms” on page 61.

Step 2: Display FPC Error Messages in the System Log File

Action To check for FPC error messages in the system log messages file, use the following CLI command:

user@host> **show log messages | match fpc**

Check for error messages at least 5 minutes before and after an FPC alarm occurs.

Sample Output The following output displays when you browse through the messages log file using the time and date stamp to look for error messages that occur 5 minutes before and after the FPC event:

```
user@host> show log messages
Mar 10 09:20:31 cls-edge-02 ssb RDP: Keepalive timeout for
rdp.(scb:chassis).(fpc1:36865) (elapsed 5595)
Mar 10 09:20:33 cls-edge-02 ssb SSB(0): Slot 0, serial number S/N BD9709.
Mar 10 09:20:37 cls-edge-02 ssb BCHIP 1: SRAM test failed.
Mar 10 09:20:37 cls-edge-02 ssb CM(0): Slot 1: B-chip diagnostics failed
Mar 10 09:20:37 cls-edge-02 ssb CM(0): Slot 1: Unrecoverable error; probe failed
Mar 10 09:20:37 cls-edge-02 ssb CM(0): Slot 1: Too many unrecoverable errors,
going off-line
Mar 10 09:20:37 cls-edge-02 ssb CM(0): ALARM SET: (Major) Slot 1: Too many
unrecoverable errors
Mar 10 09:20:37 cls-edge-02 ssb CM(0): Slot 1: Off-line
Mar 10 09:20:38 cls-edge-02 ssb PFEMAN: FPC socket closure indicated
Mar 10 09:20:38 cls-edge-02 ssb PFEMAN: closing FPC 1 socket
Mar 10 09:20:42 cls-edge-02 ssb PFEMAN: FPC socket closure indicated
Mar 10 09:20:42 cls-edge-02 ssb PFEMAN: close on unlisted socket, 0xb0e200
```

The following output displays when you use the | match filter command to look for specific information in the messages log file:

```
user@host> show log messages | match fpc
Mar 31 05:07:58 bopper fpc6 D4-6/0 AMCC: Transmitter laser bias out of range.
Mar 31 05:08:37 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 2, power on
timeout, retry 1, restarting
Mar 31 05:08:44 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 5, power on
timeout, retry 1, restarting
Mar 31 05:10:19 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 2, power on
timeout, retry 2, restarting
Mar 31 05:10:26 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 5, power on
timeout, retry 2, restarting
Mar 31 05:12:00 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 2, power on
timeout, retry 3, restarting
Mar 31 05:12:07 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: fpc 5, power on
timeout, retry 3, restarting
Mar 31 05:13:41 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: FPC 2
unresponsive, setting offline!
Mar 31 05:13:48 bopper chassisd[630]: CHASSISD_FRU_UNRESPONSIVE: FPC 5
unresponsive, setting offline!
```

What It Means When an FPC fails, the System and Switch Board (SSB), System Control Board (SCB), and Switching and Forwarding Modules (SFMs) generate error messages. The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Use the show log messages | match fpc command to view only FPC error messages. Use this information to diagnose an FPC problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events prior to the FPC problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display FPC Error Messages in the Chassis Daemon Log File

Action To display FPC error messages in the chassisd log file, use the following CLI command:

user@host> **show log chassisd | match “fpc | kernel | tnp”**

Sample Output

```
user@host> show log chassisd | match “fpc | kernel | tnp”
Nov 11 15:58:31 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=0, tnpaddr=2
Nov 11 15:58:42 m40-2 tnp.bootpd[2497]: BOOTPD_BOOTSTRING: Boot string: boot 1
fpc.jbf
Nov 11 15:58:42 m40-2 tnp.tftpd[2647]: TFTPD_CONNECT_INFO: tftp read from addr
16 port 1024 file fpc.jbf
Nov 11 15:58:42 m40-2 tnp.bootpd[2497]: BOOTPD_BOOTSTRING: Boot string: boot 1
fpc.jbf
Nov 11 15:58:43 m40-2 tnp.tftpd[2649]: TFTPD_CONNECT_INFO: tftp read from addr
17 port 1024 file fpc.jbf
Nov 11 15:58:44 m40-2 tnp.tftpd[2651]: TFTPD_CONNECT_INFO: tftp read from addr
18 port 1024 file fpc.jbf
Nov 11 15:58:45 m40-2 tnp.tftpd[2653]: TFTPD_CONNECT_INFO: tftp read from addr
19 port 1024 file fpc.jbf
Nov 11 15:58:46 m40-2 tnp.tftpd[2655]: TFTPD_CONNECT_INFO: tftp read from addr
20 port 1024 file fpc.jbf
Nov 11 15:58:47 m40-2 tnp.tftpd[2657]: TFTPD_CONNECT_INFO: tftp read from addr
21 port 1024 file fpc.jbf
Nov 11 15:58:47 m40-2 fpc6 TFTP Error - Timeout
Nov 11 15:58:47 m40-2 fpc7 TFTP Error - Timeout
Nov 11 15:58:48 m40-2 tnp.tftpd[2659]: TFTPD_CONNECT_INFO: tftp read from addr
22 port 1024 file fpc.jbf
Nov 11 15:58:49 m40-2 tnp.tftpd[2661]: TFTPD_CONNECT_INFO: tftp read from addr
23 port 1024 file fpc.jbf
Nov 11 15:58:50 m40-2 tnp.tftpd[2663]: TFTPD_CONNECT_INFO: tftp read from addr
22 port 1024 file fpc.jbf
Nov 11 15:58:50 m40-2 fpc6 TFTP read - saw block 1, expected 572
Nov 11 15:58:51 m40-2 tnp.tftpd[2665]: TFTPD_CONNECT_INFO: tftp read from addr
23 port 1024 file fpc.jbf
Nov 11 15:58:51 m40-2 fpc6 TFTP read - saw block 1, expected 731
Nov 11 15:58:51 m40-2 fpc7 TFTP read - saw block 1, expected 200
Nov 11 15:58:52 m40-2 fpc6 TFTP read - saw block 1, expected 775
Nov 11 15:58:52 m40-2 fpc7 TFTP read - saw block 1, expected 265
Nov 11 15:58:52 m40-2 tnp.tftpd[2647]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:58:53 m40-2 fpc6 TFTP read - saw block 1, expected 782
Nov 11 15:58:53 m40-2 fpc7 TFTP read - saw block 1, expected 340
Nov 11 15:58:54 m40-2 fpc7 TFTP read - saw block 1, expected 428
Nov 11 15:58:54 m40-2 fpc6 TFTP read - saw block 1, expected 1016
Nov 11 15:58:55 m40-2 fpc7 TFTP read - saw block 1, expected 531
Nov 11 15:58:57 m40-2 tnp.tftpd[2649]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
```

```
Nov 11 15:58:57 m40-2 tnp.tftpd[2651]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:58:58 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=1, tnpaddr=16
Nov 11 15:58:58 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 0 restart
Nov 11 15:59:00 m40-2 tnp.tftpd[2653]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:59:00 m40-2 tnp.tftpd[2659]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:59:01 m40-2 tnp.tftpd[2655]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:59:02 m40-2 tnp.tftpd[2661]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:59:02 m40-2 tnp.tftpd[2657]: TFTPD_SENDCOMPLETE_INFO: Sent 2335 blocks
of 1024 and 1 block of 960 for file '/usr/share/pfe/fpc.jbf'
Nov 11 15:59:03 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=2, tnpaddr=17
Nov 11 15:59:03 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 1 restart
Nov 11 15:59:03 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=3, tnpaddr=18
Nov 11 15:59:03 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 2 restart
Nov 11 15:59:06 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=4, tnpaddr=19
Nov 11 15:59:06 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 3 restart
Nov 11 15:59:07 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=5, tnpaddr=22
Nov 11 15:59:07 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 6 restart
Nov 11 15:59:07 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=6, tnpaddr=20
Nov 11 15:59:08 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 4 restart
Nov 11 15:59:08 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=7, tnpaddr=23
Nov 11 15:59:08 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 7 restart
Nov 11 15:59:09 m40-2 /kernel: pfe_listener_connect: conn established: listener
idx=8, tnpaddr=21
Nov 11 15:59:09 m40-2 chassisd[2476]: CHASSISD_EVENT: fpc slot 5 restart
```

What It Means The chassisd log file is a database that provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. The sample command output shows the results of a multiple item search in the log file ("fpc | kernel | tnp"): error messages for the FPC, kernel, and Trivial Networking Protocol (TNP) that indicate communication issues between the Routing Engine and the Packet Forwarding Engine components.

Verifying FPC Failure

Action To verify an FPC failure, follow these steps:

Step 1: Document Events Prior to the FPC Failure

Action To document an FPC failure, record any events that may have led to the FPC failure, such as a software upgrade, hardware upgrade, or a reset. Capture system log file error messages 5 minutes before and after a failure event by using the show log messages command and use the time and date stamp to browse the file. You can use the show log messages | match command to view certain common error messages and help identify why an FPC failure occurred.

Step 2: Check the FPC Installation

Action To check the FPC installation and verify an FPC failure, follow these steps:

1. Make sure that the FPC is seated in its slot. Use a screwdriver to check that the screws at the top and bottom of the card carrier are tight.
2. Try to bring the FPC online. Press the online button on the craft interface or FPM for a few seconds. If the FPC does not come online, it has probably failed.
3. If the FPC comes online, check the FPC detailed status with the following CLI command:

   user@host> **show chassis fpc detail** *fpc-slot*

Alternative Action For the M40e, M160, M320 and T320 routers and T640 routing node, to bring the FPC online, use the request chassis fpc *slot-number* online command.

Step 3: Check the FPC Fuses

The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly. You must remove the lower impeller assembly to access the fuses, as described in the appropriate hardware guide.

The M320 router requires fuses for the FPCs. The fuses for the and FPCs are located in the rear of the midplane behind the power supply in slot PEM0.

When the fuse for an FPC blows, the FPC stops functioning even though it is installed correctly and the power supplies are providing power to the router.

For the M40e and M160 routers, when a fuse has blown but the power supplies are still delivering power to router, the amber LED adjacent to the fuse lights. For vertically oriented fuses (in the groups labeled J241 through J244.

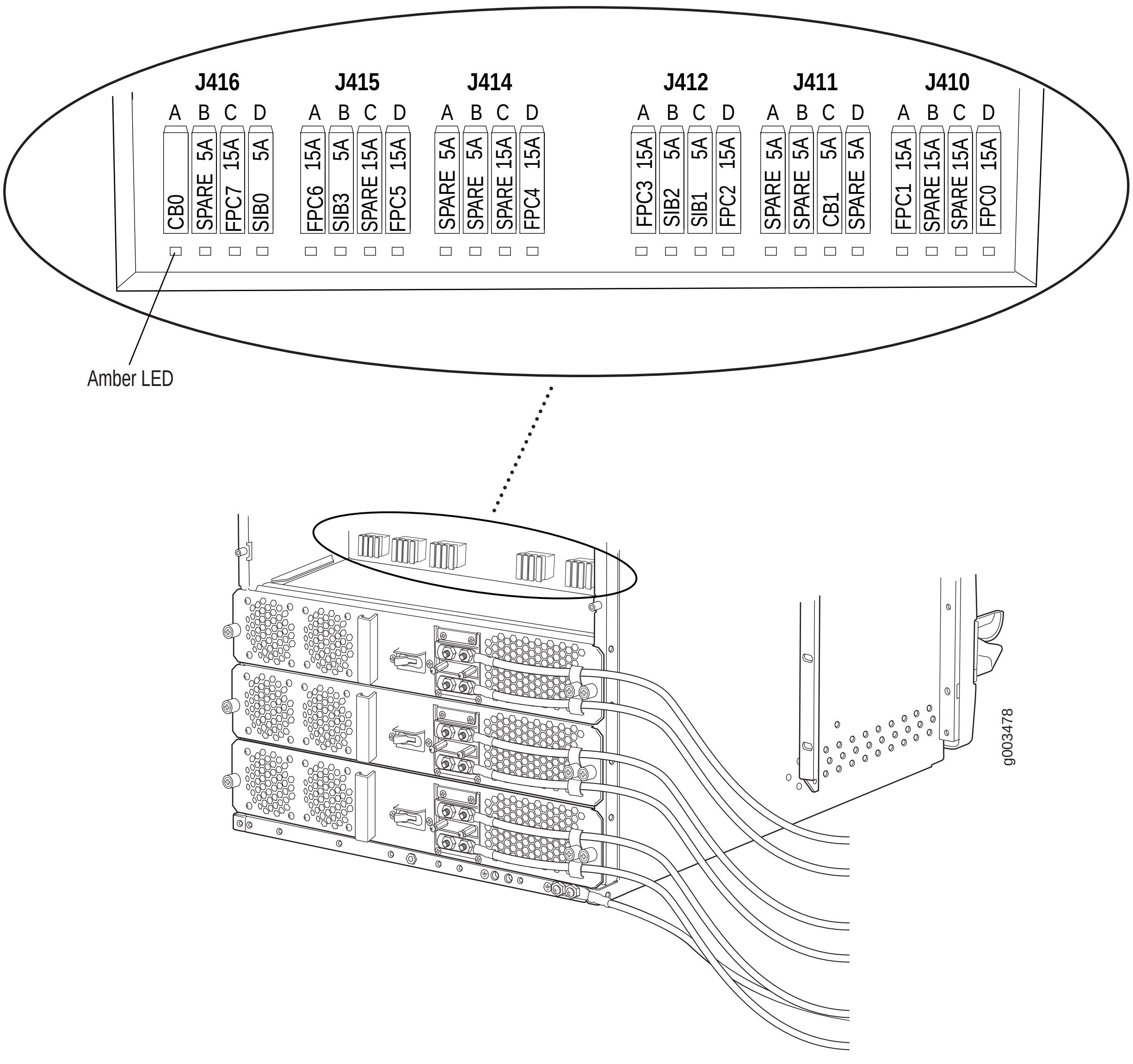
Another indication that a fuse has blown is when the colored indicator bulb inside it becomes visible through the clear cover on the fuse. For information about the indicator bulb color for each fuse type, see the appropriate router hardware guide.

A blown fuse can cause a component to fail even though it is correctly installed and the power supplies are functioning. Check for a blown fuse in the following circumstances:

- The LED that indicates normal operation for the component fails to light.
- The appropriate CLI show chassis environment command indicates that the component is installed but is not receiving power.

Figure 58 shows the location of the M320 fuses in the rear of the midplane for the FPC. (The labels shown in the figure do not appear on the actual fuses—the clear cover on every fuse reads BUSS GMT-X—and might not match the labels on the midplane. Ignore the labels on the midplane.)

Figure 58: Component Fuses in the M320 Router Midplane



Step 4: Take the FPC Offline

The FPCs are hot-insertable and hot-removable. When you remove an FPC, the router continues to function, although the PIC interfaces installed on the FPC no longer function.

Action To take an FPC offline, press the offline button for approximately 3 seconds, and follow the instructions in the appropriate router hardware guide.

Step 5: Perform an FPC Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the FPC for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an FPC, follow these steps:

1. Remove the FPC that you suspect has failed from the router chassis.
2. Inspect the router midplane for bent pins. Inspect the FPC connector for pins that are stuck. If you find a bent or stuck pin, see "Return the Failed Component" on page 86.
3. If there are no bent or stuck pins and there is a spare FPC slot in the router, insert the FPC that failed into a spare slot. If the FPC still fails, see "Return the Failed Component" on page 86. If there is no spare FPC slot, insert an FPC that you know works into the slot where the FPC failed. If the FPC works, the replaced FPC failed. If the FPC does not work, the FPC slot has failed.

Step 6: Display the FPC Software Version Information

Action To display the version of kernel software running on the router, use the following CLI command:

user@host> **show version brief**

Sample Output

```
user@host> show version brief
Hostname: host
Model: m160
JUNOS Base OS boot [5.5R1.2]
JUNOS Base OS Software Suite [5.5R1.2]
JUNOS Kernel Software Suite [5.5R1.2]
JUNOS Packet Forwarding Engine Support [5.5R1.2]
JUNOS Routing Software Suite [5.5R1.2]
JUNOS Online Documentation [5.5R1.2]
JUNOS Crypto Software Suite [5.5R1.2]
```

What It Means The command output displays the router hostname, model number, and the version of software running on the router. The kernel software version is important when diagnosing FPC issues. You will need this information when you contact JTAC.

Step 7: Display the FPC Hardware Information

Action To display the FPC hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
[...Output truncated...]
FPC 0            REV 01   710-001292   AE3843
  PIC 0          REV 04   750-000617   AE2495            1x OC-48 SONET, SMIR
FPC 1            REV 07   710-000175   AA3408
  PIC 0          REV 01   750-001323   AB1244            1x Tunnel
  PIC 1          REV 05   750-000613   AA3151            1x OC-12 SONET, SMIR
FPC 3            REV 01   710-000175   AA0048
  PIC 0          REV 04   750-000613   aa0343            1x OC-12 SONET, SMIR
  PIC 1          REV 05   750-000616   AA1394            1x OC-12 ATM, MM
  PIC 2          REV 04   750-000613   AA0377            1x OC-12 SONET, SMIR
  PIC 3          REV 04   750-000613   AA0378            1x Tunnel
FPC 5            REV 07   710-000175   AA3475
  PIC 0          REV 04   750-000611   AA3506            4x OC-3 SONET, MM
  PIC 2          REV 06   750-001072   AA1785            1x G/E, 1000 BASE-SX
FPC 7            REV 07   710-000175   AA3409
  PIC 1          REV X1   750-000603   AA0181            4x OC-3 SONET, SMIR
```

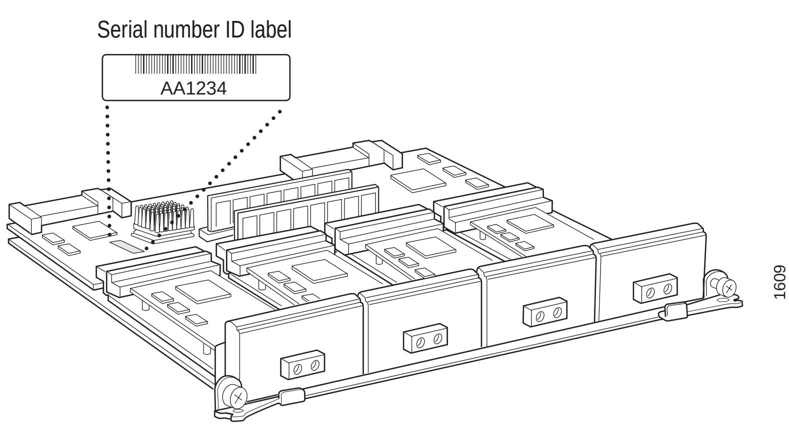
What It Means The command output displays each FPC installed in the router, including the version level, part number, serial number, and description. The output also displays a description of the PICs installed in each FPC. You will need this information when you contact JTAC.

Step 8: Locate the FPC Serial Number ID Label

Action The serial number ID label is small, rectangular, and has the component serial number and bar code on it. To locate the FPC serial number ID label, do one of the following:

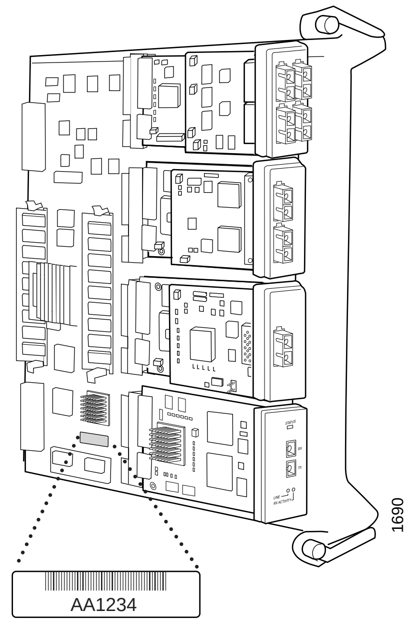
- M20 router—With the FPC in horizontal position, look on the top back right of the FPC (see Figure 59).

Figure 59: M20 Router FPC Serial Number ID Label



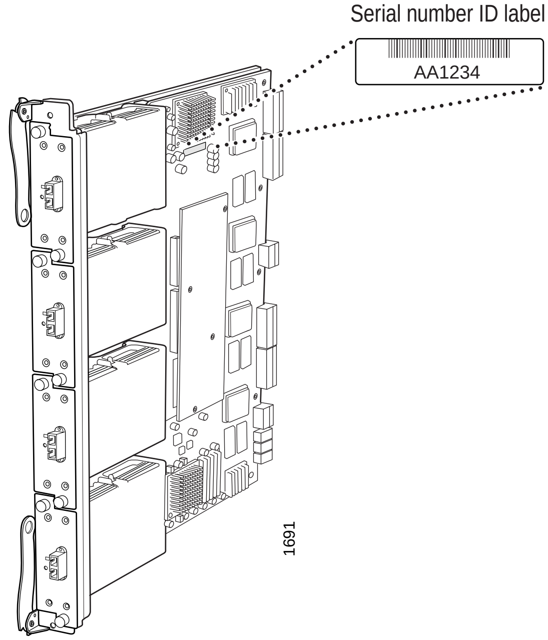
- M40 router—With the FPC in vertical position, look on the back left side of the FPC (see Figure 60).

Figure 60: M40 Router FPC Serial Number ID Label



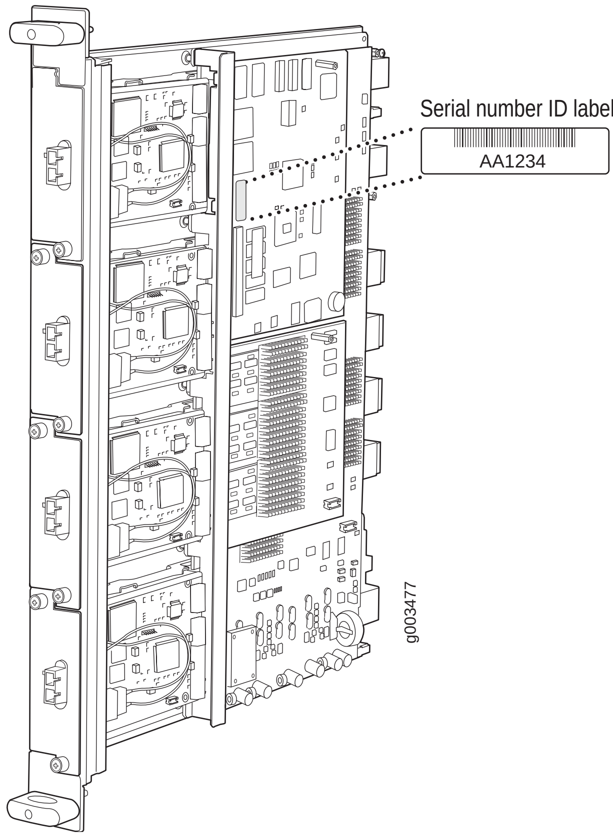
- M40e and M160 routers—With the FPC in vertical position, look on the center right side of the FPC (see Figure 61).

Figure 61: M40e and M160 Router FPC Serial Number ID Label



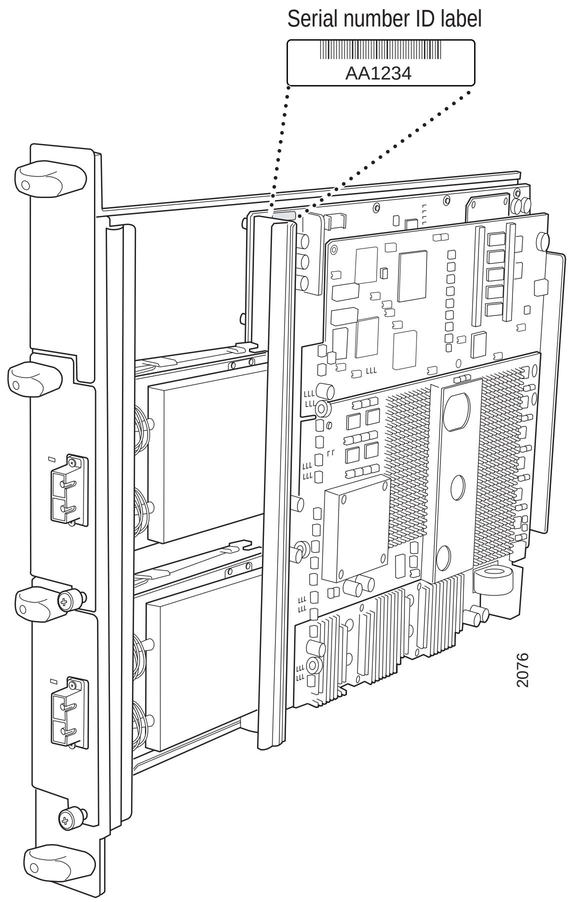
- M320 routers—The serial number ID label is located on the center of the right side of the FPC3 (see Figure 62). On an FPC2, the serial number label is located on the top PIC slot.

Figure 62: M320 FPC Serial Number ID Label



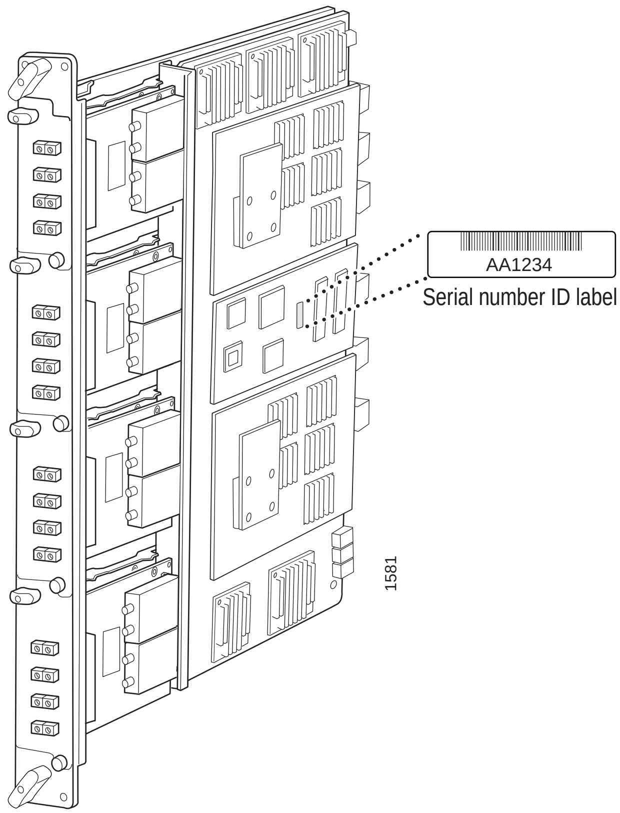
- T320 routers—The serial number ID label is located on the center of the right side of the FPC3 (see Figure 63). On an FPC1 and FPC2, the serial number ID label is located near the top PIC slot.

Figure 63: T320 Router FPC Serial Number ID Label



- T640 routing nodes— The serial number label is located on the center of the right side of the FPC3 (see Figure 64). On an FPC2, the serial number label is located near the top PIC slot.

Figure 64: T640 Routing Node Serial Number Label



Replacing an FPC

The FPC is hot-removable and hot-insertable. You can remove or replace it without powering down the router and disrupting routing functions. However, you must first take the FPC offline by pressing the FPC offline button on the router craft interface for all router platforms except the M5 and M10 routers.

Action To return a failed FPC, see “Return the Failed Component” on page 86. To replace an FPC, see the appropriate router hardware guide.

Chapter 16

Monitoring PICs

You monitor and maintain Physical Interface Cards (PICs) to ensure that they receive incoming packets from the network and transmit outgoing packets to the network. (See Table 48.)

Table 48: Checklist for Monitoring PICs

Monitor PIC Tasks	Command or Action
Understanding PICs on page 184	
■ PIC Location, Row, and Slot Numbering on page 185	
Checking the PIC Status on page 186	
1. Display the PIC Media Type and FPC Status on page 186	show chassis fpc pic-status show chassis pic pic-slot # fpc-slot #
2. Display the PIC Interface Status Information on page 187	show interfaces terse
3. Check the PIC LED States on page 188	Check the PIC port LEDs.
Checking PIC Alarms on page 189	
1. Check Current Chassis Alarms on page 189	show chassis alarms show chassis craft-interface
2. Display Error Messages in the System Log File on page 190	show log messages | match PIC
Verifying PIC Failure on page 190	
1. Perform a PIC Swap Test on page 190	Replace the PIC with one that you know works, then use the show chassis fpc pic-status command.
2. Display PIC Hardware Information on page 191	show chassis hardware
3. Locate the PIC Serial Number ID Label on page 192	Look on the right side of the top of the PIC if horizontally oriented. Look on the left side of the PIC if vertically oriented.
Replacing a PIC on page 195	See "Return the Failed Component" on page 86. Follow the procedure in the appropriate router hardware guide. See also the appropriate PIC guide.

Understanding PICs

Purpose Inspect PICs to ensure that data packets are received from and transmitted to the network for supported media types.

What Is a PIC A PIC is an interface card through which network cables carry data transmissions to and from the network plug. A PIC installs into a Flexible PIC Concentrator (FPC).

PICs are hot-removable and hot-insertable. Removing or inserting a PIC causes a brief interruption of forwarding performance. Each PIC has an ejector lever at the bottom of its faceplate that allows for easy removal from the router.

Table 49 lists some PIC characteristics for each routing platform. A PIC performs framing and line-speed signaling for its media type.

Table 49: PIC Characteristics Per Routing Platformj

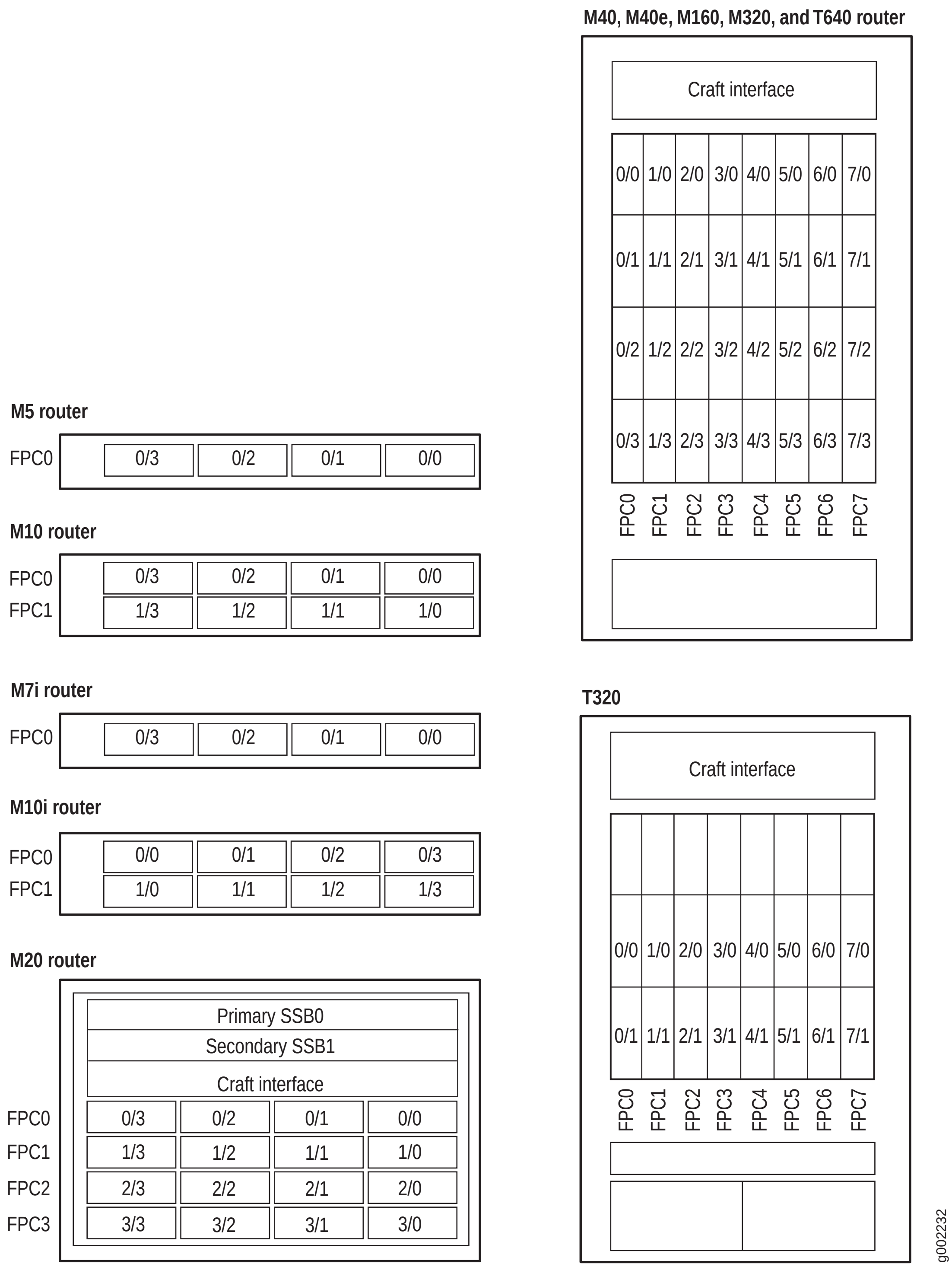
PIC Characteristic	M5/ M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
Single-wide PICs per FPC	4/8	4	8	16	32	32	32	32	16 (2 PICs per FPC)	32
Accepts Quad-wide PIC	Yes, M10 Internet router only		Yes	Yes, FPC not required	Yes, FPC not require d	No	Yes, FPC not require d	N/A 2 PICs per FPC3	N/A	N/A

Before transmitting outgoing data packets, the PICs encapsulate packets received from the FPCs. Each PIC is equipped with an application-specific integrated circuit (ASIC) that performs control functions specific to the PIC's media type.

For a listing of PICs supported for each routing platform, see the appropriate router hardware guide and the router PIC guide.

Figure 65 on page 185 shows the PIC location in each router and the corresponding row and slot numbering.

Figure 65: PIC Location, Row, and Slot Numbering



See Also "Monitoring FPCs" on page 163

Checking the PIC Status

Steps To Take To check the PIC status, follow these steps:

1. Display the PIC Media Type and FPC Status on page 186
2. Display the PIC Interface Status Information on page 187
3. Check the PIC LED States on page 188

Step 1: Display the PIC Media Type and FPC Status

Action To display the PIC media type and FPC status, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis fpc pic-status**

Sample Output

```
user@host> show chassis fpc pic-status
Slot 0 Online
  PIC 0    1x OC-12 SONET, MM
  PIC 1    4x OC-3 SONET, SMIR
  PIC 2    4x E1, BNC
  PIC 3    1x CSTM1, SMIR
Slot 1 Online
  PIC 0    4x CT3
Slot 2 Online
  PIC 0    1x Tunnel
Slot 4 Online
Slot 5 Offline
Slot 6 Online
  PIC 0    1x OC-192 12xMM VSR
```

What It Means The command output displays the status for all FPCs installed in the router and a description of the PICs installed in each FPC, including the number of ports, media type, mode, and reach. The FPCs in slots 0, 1, 2, 4, and 6 are online. The FPC in slot 5 is offline. The PICs installed in the router include SONET, E1, Channelized STM1, CT3, Tunnel, and OC192 media PICs.

In the example, PIC 0 is one-port, SONET, OC12, and multimode.

For more detailed information about PIC types, see the appropriate router PIC guide.

Alternative Actions To check PIC status including port information, use the show chassis pic pic-slot # fpc-slot # CLI command. The command output for an M10i router displays the PIC type, ASIC type, operating status, PIC version, and how long the PIC has been online. Additionally, the command output displays the PIC port number, type, small form-factor pluggable transciever (SFP) vendor, and part number information.

user@host> **show chassis pic pic-slot 0 fpc-slot 1**

Sample Output

```
user@host> show chassis pic pic-slot 0 fpc-slot 1
PIC fpc slot 1 pic slot 0 information:
  Type                             1x OC-48 SONET SFP
  ASIC type                        D chip
  State                            Online
  PIC version                  1.1
  Uptime                        7 days, 13 hours, 29 minutes, 51 seconds

PIC Port Information:
  Port        Cable             SFP                 SFP Vendor
  Number      Type              Vendor Name         Part Number
  0           OC48 SHORT REACH  SumitomoElectric    SCP6828-J1-ANE
  1           UNKNOWN CABLE
  2           UNKNOWN CABLE
  3           UNKNOWN CABLE
```

To check the PIC media type and status for a particular FPC, use the show chassis fpc pic-status *fpc-slot* command.

To display PIC hardware information, including the media type description, use the show chassis hardware command.

Syntax

show chassis fpc <pic-status <*fpc-slot*>>
show chassis hardware

Step 2: Display the PIC Interface Status Information

Action

To display the status of each configured interface, use the following JUNOS CLI operational mode command:

user@host> **show interfaces terse**

Sample Output

```
user@host> show interfaces terse
Interface       Adman Link Port Local            Remote
so-0/0/0        up    up
so-0/0/0.0      up    up   inet  192.168.36.201      --> 192.168.36.200
so-0/1/0        up    down
so-0/1/1        up    down
e1-0/2/0        up    down
e1-0/2/1        up    down
t1-1/0/0:1      up    down
t1-1/0/0:2      up    down
gr-2/0/0        up    up
ip-2/0/0        up    up
[...Output truncated...]
```

What It Means

The command output shows the names of all interfaces configured on the router. The interface name indicates the *media type-fpc/pic/port* (for example, so-0/0/0.0). It shows whether the interface is on (up) or off (down) and whether the link state is up or down. Additionally, the output shows the protocol configured on that interface and the local address of the interface, as well as the address of the remote side of a connection for point-to-point interfaces. Refer to the PIC for port numbering.

A line in the sample output shows the status of a SONET interface on FPC 0, PIC 0, port 0, and logical unit number 0. The status of the interface is up. The link status is up. The protocol configured on the interface is inet. The local interface IP address is 192.168.36.201 and the remote IP address is 192.168.36.200.

The interface is configured with a /32 subnet. If you configure the interface with a different subnet, the output will be different.

For more detailed information about monitoring interfaces, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

Alternative Actions To view more detailed information about a particular interface, use the show interfaces *interface-name* brief command. The command output shows the interface status, link-level type, loopback, device flags, interface flags, keepalive settings, keepalive input, active alarms, and defects.

To view interface status information, use the show interface descriptions command. This command displays the interface status and the description given when configured on the router.

Syntax show interfaces terse <*interface-name*>
show interfaces <*interface-name*> brief

Step 3: Check the PIC LED States

For PICs that have a physical port, the LEDs indicate the status of the physical link. If the LED is green, the physical link is up. If the LED is red or amber, the physical link is down. Usually, when the LED is red, the receive port is not receiving a signal. If the LED is amber, the receive port is getting a remote alarm from the device.

For PICs with no physical port, such as a tunnel or encryption PIC, the LED indicates the status of the PIC.

The Tunnel PIC, which has no ports, has a single LED. Each LED has four different states, described in Table 50.

Table 50: Tunnel PIC LEDs

Color	State	Description
Red	Fail	The FPC has detected a PIC failure.
Green	Normal	The port is functioning normally.
Amber	Problem detected; still functioning	To track the problem, use the CLI.
None	Not enabled	The port is not enabled or the PIC is offline.

For M7i and M10i routers, most PICs have an LED labeled STATUS on the PIC faceplate. Some PICs have additional LEDs, often one per port. The meaning of the LED states differs for various PICs. For more information, see the appropriate router PIC guide.

Checking PIC Alarms

Steps To Take To check for PIC alarms, follow these steps:

1. Check Current Chassis Alarms on page 189
2. Display Error Messages in the System Log File on page 190

Step 1: Check Current Chassis Alarms

Action To display current PIC alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time              Class  Description
2002-04-08 10:01:20 PDT  Major  PIC 0/2 failed to initialize
```

What It Means The command output displays the alarm time, severity level, and description.

Alternative Action You can also display PIC alarms by using the following CLI command:

user@host> **show chassis craft-interface**

```
user@host> show chassis craft-interface
Red alarm:     LED on, relay on
Yellow alarm:  LED off, relay off
Host OK LED:   On
Host fail LED: Off

FPCs     0  1  2  3  4  5  6  7
-------------------------------
Green    *  .  .  *  .  .  .  .
Red      .  .  .  .  .  .  .  .

LCD screen:
     +--------------------+
     |myrouter            |
     |1 Alarm active      |
     |R: PIC 0/2 FAILED   |
     |                    |
     +--------------------+
```

Step 2: Display Error Messages in the System Log File

Action To display PIC error messages in the system log file, use the following CLI command:

user@host> **show log messages | match PIC**

Sample Output

```
user@host> show log messages | match PIC
Apr  8 10:01:20 aspirin scb CM: PIC 0/2, ID 0x0206, hardware error, offlined
Apr  8 10:01:20 aspirin alarmd[2671]: Alarm set: FPC color=RED, class=CHASSIS,
reason=PIC 0/2 failed to initialize
Apr  8 10:01:20 aspirin fpc0 PIC: PIC 2 discovery error (1)
Apr  8 10:01:20 aspirin fpc0 CMFPC: Hardware error discovering PIC 2, ID 0x0206
Apr  8 10:01:21 aspirin scb CM: ALARM SET: (Major) Slot 0: PIC 0/2 failed to
initialize
```

What It Means When a PIC fails, the messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Use the show log messages command to browse error messages that are generated at least 5 minutes before and after a PIC event. You can also use the show log messages | match PIC command to view specific PIC error messages with common information. Use this information to diagnose a PIC problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events prior to the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Verifying PIC Failure

Steps To Take To verify PIC failure, follow these steps:

1. Perform a PIC Swap Test on page 190
2. Display PIC Hardware Information on page 191
3. Locate the PIC Serial Number ID Label on page 192

Step 1: Perform a PIC Swap Test

Action To perform a swap test on a PIC, follow these steps:

1. Ensure that the PIC is firmly seated in the FPC or the FPC slot.
2. If the PIC is firmly seated and still fails, remove it from the FPC. Follow the PIC removal procedure in the appropriate router PIC guide.

3. Check the PIC connector pins.

   a. If a pin is bent, contact JTAC and generate a Return Material Authorization (RMA). For more information about returning a failed router part, see “Return the Failed Component” on page 86.

   b. If no pins are bent, install a PIC that you know works into the FPC.

   c. Check the PIC status by looking at the PIC LEDs and using the show chassis fpc pic-status command (see “Display the PIC Media Type and FPC Status” on page 186).

4. If the PIC works, then the PIC you removed is defective. Contact JTAC and generate an RMA. See “Return the Failed Component” on page 86.

Step 2: Display PIC Hardware Information

Action To display PIC hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
[...Output truncated...]
FPC 0            REV 03   710-001255   S/N AA9806       FPC Type 1
  CPU            REV 02   710-001217   S/N AA9590
  PIC 1          REV 05   750-000616   S/N AA1527       1x OC-12 ATM, MM
  PIC 2          REV 05   750-000616   S/N AA1535       1x OC-12 ATM, MM
  PIC 3          REV 01   750-000616   S/N AA1519       1x OC-12 ATM, MM
FPC 1            REV 02   710-001611   S/N AA9523       FPC Type 2
  CPU            REV 02   710-001217   S/N AA9571
  PIC 0          REV 03   750-001900   S/N AA9626       1x STM-16 SDH, SMIR
  PIC 1          REV 01   710-002381   S/N AD3633       2x G/E, 1000 BASE-SX
FPC 2                                                   FPC Type OC192
  CPU            REV 03   710-001217   S/N AB3329
  PIC 0          REV 01                                 1x OC-192 SM SR-2
```

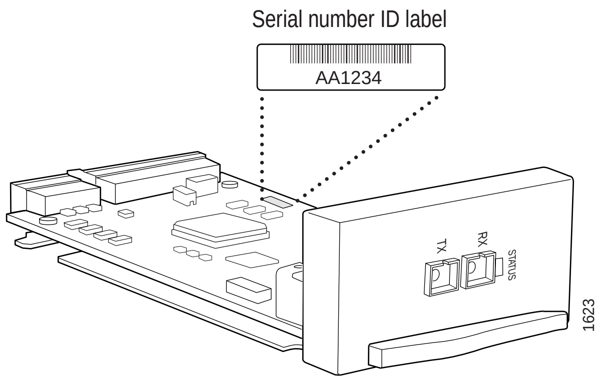
What It Means The command output displays the PIC number, revision level, part number, serial number, and media type.

Step 3: Locate the PIC Serial Number ID Label

Action To locate the PIC serial number ID label, do one of the following:

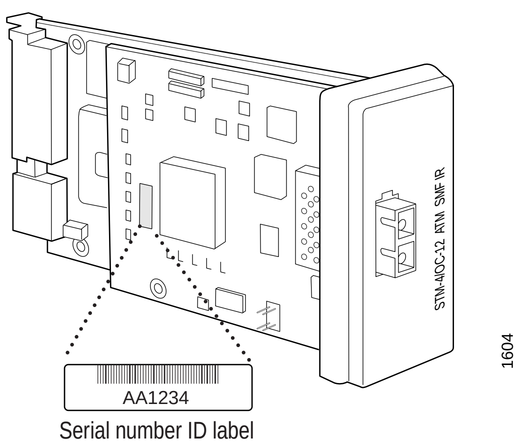
- With the PIC in horizontal position, look on the right side of the top of the PIC (see Figure 66).

Figure 66: PIC Serial Number ID Label (Horizontal Orientation)



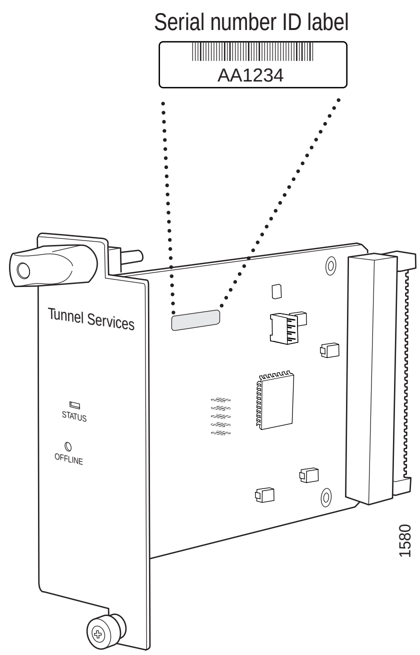
- With the PIC in vertical position, look on the left side of the PIC (see Figure 67).

Figure 67: PIC Serial Number ID Label (Vertical Orientation)



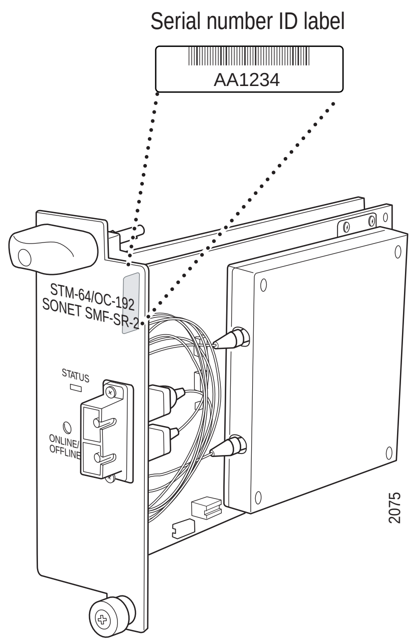
For M320 routers, the serial number ID label is located on the right side of the PIC (see Figure 68) when the PIC is vertically oriented (as it would be installed in the router). The exact location may be slightly different on different PICs, depending on the placement of components on the PIC board.

Figure 68: M320 Router Serial Number ID Label on PIC



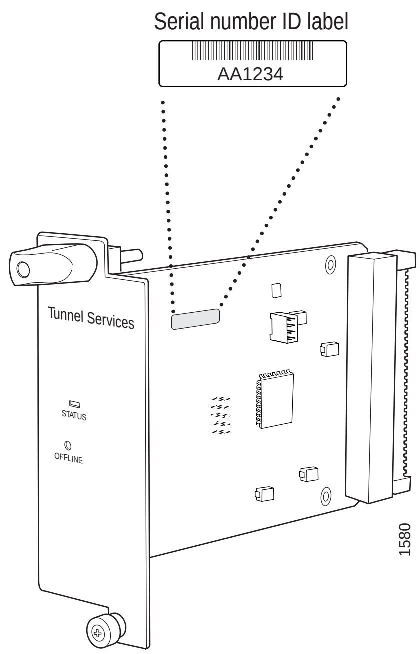
For T320 routers, the serial number ID label is located on the right side of the PIC (see Figure 69) when the PIC is vertically oriented (as it would be installed in the router). The exact location may be slightly different on different PICs, depending on the placement of components on the PIC board.

Figure 69: T320 Router Serial Number ID Label on PIC



For T640 routing nodes, the serial number label is located on the right side of the PIC (see Figure 70) when the PIC is vertically oriented (as it would be installed in the routing node). The exact location may be slightly different on different PICs, depending on the placement of components on the PIC board.

Figure 70: T640 Routing Node Serial Number Label on PIC



Replacing a PIC

Action To remove a PIC, refer to the appropriate PIC guide.

For information about returning a PIC, see "Return the Failed Component" on page 86. To replace a PIC, see the appropriate router hardware guide or PIC guide.

Chapter 17

Monitoring the Craft Interface

You monitor and maintain the craft interface or Front Panel Module (FPM) to ensure that you can view the router status and perform management operations from the panel on the front of the chassis. (See Table 51.) You can also display craft interface information from the JUNOS software command-line interface (CLI).

Table 51: Checklist for Monitoring the Craft Interface

Monitor Craft Interface Tasks	Command or Action
Understanding the Craft Interface on page 199	
■ M5 and M10 Router Craft Interface on page 199 ■ M20 Router Craft Interface on page 200 ■ M40 Router Craft Interface on page 200 ■ M40e and M160 Router Craft Interface on page 201 ■ M320 Router Craft Interface on page 201 ■ T320 Router and T640 Routing Node Craft Interface on page 202	
Monitoring the Craft Interface Status on page 203	
1. View the Craft Interface Status on page 203	show chassis craft interface Physically check the craft interface panel.
2. Check the Craft Interface Environmental Status on page 203	show chassis environment (M40e, M160, and T320 routers and T640 routing node only) show chassis environment fpm
Viewing Craft Interface Information from the Command Line on page 204	show chassis craft-interface
Verifying Craft Interface Failure on page 205	
1. Display Craft Interface Alarms on page 206	show chassis alarms
2. Display Craft Interface Error Messages in the System Log File on page 207	show log messages
3. Display Craft Interface Messages in the Chassis Daemon Log File on page 208	show log chassisd
4. Display Craft Interface Hardware Information on page 208	show chassis hardware

Monitor Craft Interface Tasks	Command or Action
Replacing the Craft Interface on page 209	
1. Replace the M20 Router Craft Interface on page 209	1. Attach an ESD wrist strap to your wrist. 2. Unscrew the thumbscrews on the left and right sides of the craft interface. 3. Flip the ends of the two extractor clips towards the outside edges of the router. 4. Grasp both sides of the craft interface and slide it out of the chassis.
2. Replace the M40 Router Craft Interface on page 209	The craft interface is attached to the lower impeller tray. 1. Attach an ESD wrist strap to your wrist. 2. Unscrew the three screws at the bottom edge of the lower impeller tray. 3. Grasp the sides of the lower impeller tray, and slide it out of the chassis.
3. Replace the M40e and M160 Router Craft Interface on page 210	The craft interface is attached to the upper impeller assembly (front top blower). 1. Attach an ESD wrist strap to your wrist. 2. Undo the captive screws at the corners of the craft interface. 3. Grasp the craft interface and pull it out of the chassis.
4. Replace the M320 Router Craft Interface on page 211	The craft interface is located on the front of the chassis above the FPC card cage.
5. Replace the T320 Router and T640 Routing Node Craft Interface on page 212	The craft interface is located on the front of the chassis above the FPC card cage.
Locating the Craft Interface Serial Number ID Label on page 213	
1. Locate the M20 Router Craft Interface Serial Number ID Label on page 213	Remove the craft interface and look for the serial number ID label on the back of the unit.
2. Locate the M40 Router Craft Interface Serial Number ID Label on page 214	Remove the craft interface and look for the serial number ID label on the back of the unit.
3. Locate the M40e and M160 Router Craft Interface Serial Number ID Label on page 214	Remove the craft interface and look for the serial number ID label on the back of the unit.
4. Locate the M320 Router Craft Interface Serial Number ID Label on page 215	Remove the craft interface and look for the serial number ID on the back of the unit, behind the alarm LEDs.
5. Locate the T320 Router and T640 Routing Node Craft Interface Serial Number ID Label on page 215	Remove the craft interface and look for the serial number ID label on the back of the unit.
Returning the Craft Interface on page 215	See “Replacing a Failed Component” on page 122, or follow the procedure in the appropriate router hardware guide.

Understanding the Craft Interface

Purpose Inspect the craft interface to ensure that you can monitor the status of the router and perform system management functions. The craft interface is also referred to as the Front Panel Module (FPM).

What Is the Craft Interface The craft interface, located on the front of the router chassis, provides status information, alarm indicators and contacts, Physical Interface Card (PIC) online and offline buttons, Flexible PIC Concentrator (FPC) online and offline buttons and LED status indicators, Routing Engine offline button and LED status indicators, and management access to the router.

You can display craft interface status information from the JUNOS software CLI.

The craft interface is hot-removable and hot-insertable. You can remove and replace it without powering down the router or disrupting routing functions.

For detailed information about how the router craft interface works, see the appropriate router hardware guide.

Figure 71 shows the M5 and M10 Internet router craft interface.

Figure 71: M5 and M10 Router Craft Interface

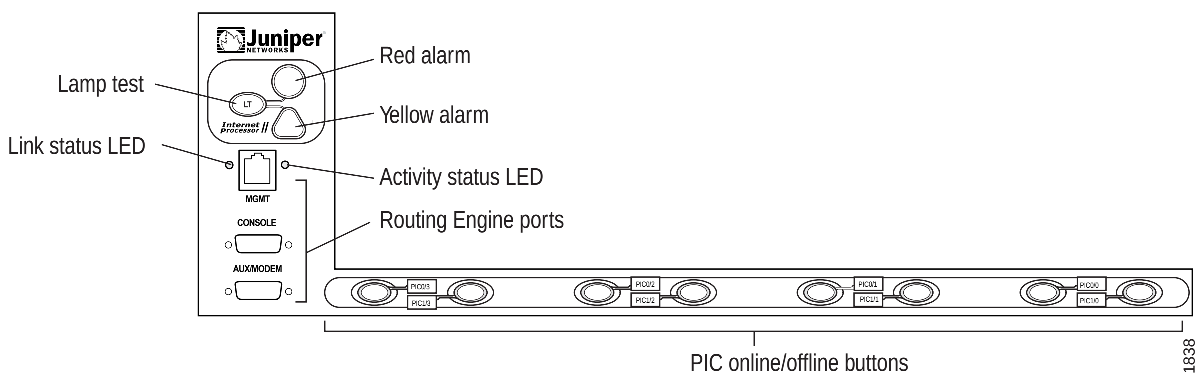


Figure 72 shows the M20 Internet router craft interface.

Figure 72: M20 Router Craft Interface

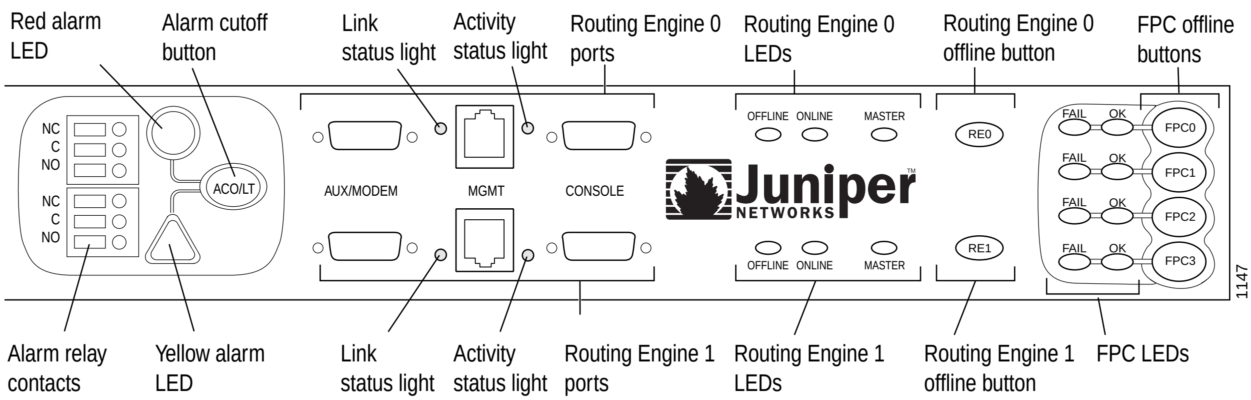


Figure 73 shows the M40 Internet router craft interface.

Figure 73: M40 Router Craft Interface

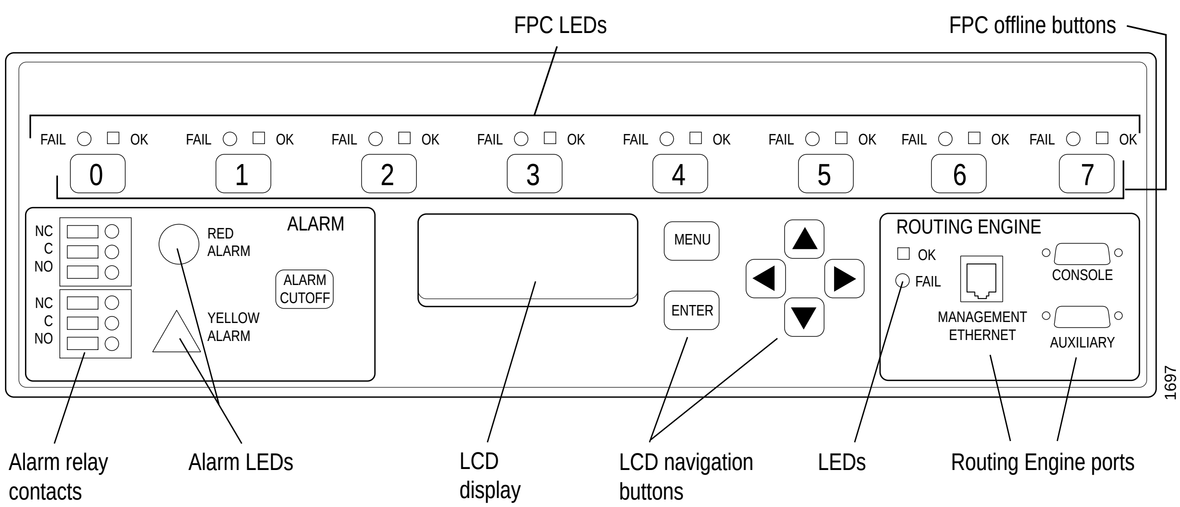


Figure 74 shows the M40e and M160 Internet router craft interface.

Figure 74: M40e and M160 Router Craft Interface

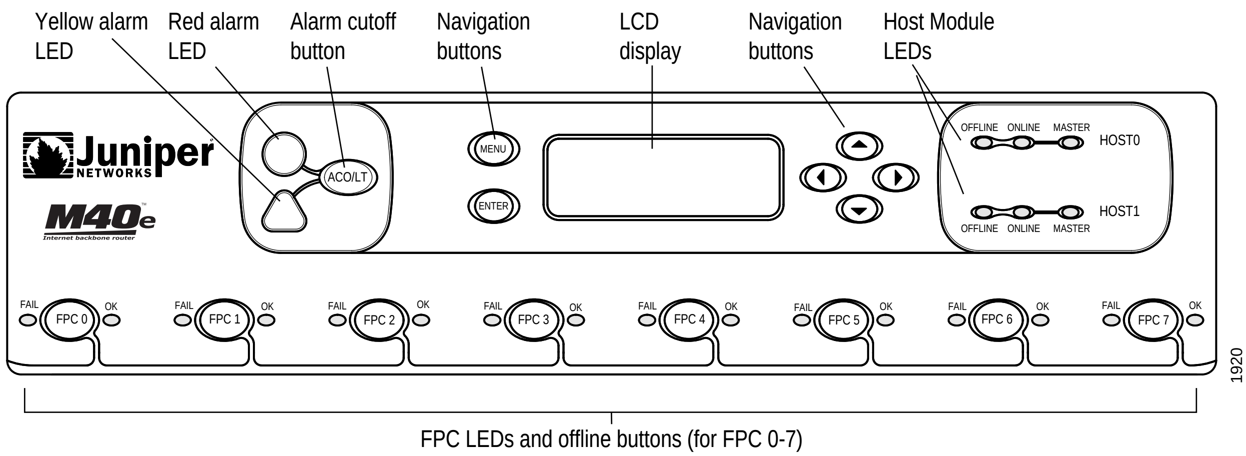


Figure 76 shows the M320 Internet router craft interface.

Figure 75: M320 Router Craft Interface

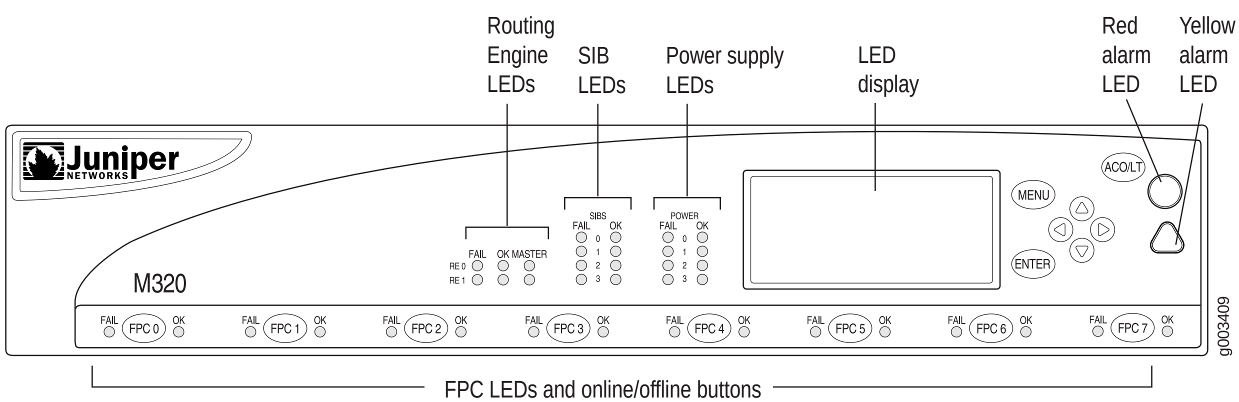


Figure 76 shows the T320 Internet router and T640 Internet routing node craft interface.

Figure 76: T320 Router and T640 Routing Node Craft Interface

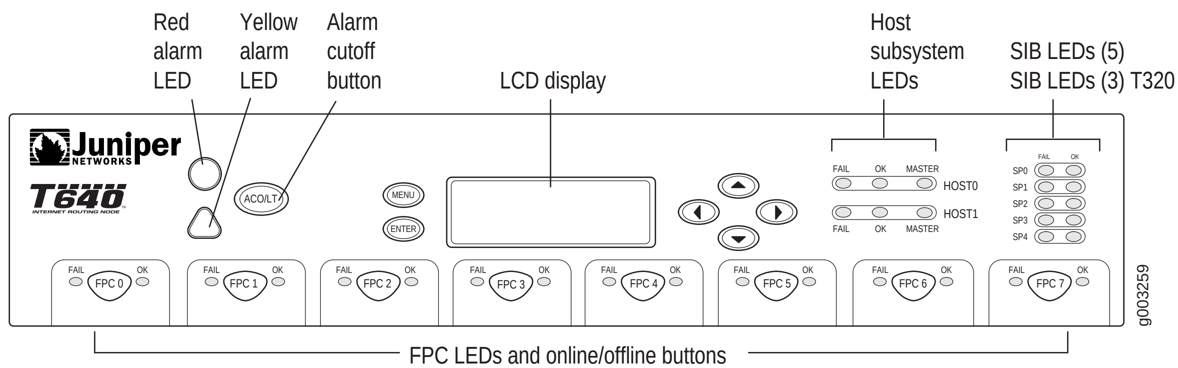


Table 52 lists the craft interface characteristics for each routing platform.

Table 52: Router Craft Interface Characteristics Per Routing Platform

Characteristic	M5 /M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
Alarm LEDs	X	X	X	X	X	X	X	X	X	X
Lamp test button	X									
Alarm cutoff button				X		X	X	X	X	X
Alarm relay contacts				X	X					
Link and activity status lights	X	X		X						
LCD display and navigation buttons					X	X	X	X	X	X
Routing Engine ports	X			X	X					
Routing Engine LEDs	No Craft Interface	No Craft Interface	No Craft Interface	X	X			X		
Host module LEDs						X	X			
Switch Interface Board (SIB) LEDs								X		
Host subsystem LEDs									X	X
PIC online and offline buttons	X	X	X							
FPC LEDs				X	X	X	X	X	X	X
FPC offline buttons				X						
Power Supply LEDs								X		
HCM LEDs			X							

See Also "Monitoring the Router Chassis" on page 107

"Monitoring the CIP" on page 381

Monitoring the Craft Interface Status

Steps To Take To monitor the craft interface status, follow these steps:

1. View the Craft Interface Status on page 203
2. Check the Craft Interface Environmental Status on page 203

Step 1: View the Craft Interface Status

Action To view the craft interface status, look at the craft interface panel on the front of the router chassis. (See Figure 71 on page 199 through Figure 76 on page 202.)

When the craft interface fails, you might not see any lights on the craft interface panel and the LCD display will be blank. In addition, the buttons on the panel might not work as indicated.

Alternative Action You can view the craft interface information with the following CLI command:

user@host> **show chassis craft-interface**

If the craft interface fails, you can still view current craft interface information at the command line. A craft interface failure or removal generates a red alarm. See “Viewing Craft Interface Information from the Command Line” on page 204.

Step 2: Check the Craft Interface Environmental Status

Action To check the craft interface status, use the following CLI command:

user@host> **show chassis environment**

Sample Output For M5, M10, M20, and M40 routers:

```
user@host> show chassis environment
Class Item                   Status     Measurement
[...Output truncated...]
Misc  Craft Interface        OK
```

For M40e and M160 routers:

```
user@host> show chassis environment
Class Item                   Status     Measurement
[...Output truncated...]
      FPM CMB                OK         32 degrees C / 89 degrees F
      FPM Display            OK         32 degrees C / 89 degrees F
[...Output truncated...]
```

For M40e and M160 routers:

```
user@host> show chassis environment
Class Item                   Status     Measurement
[...Output truncated...]
      FPM GBUS               OK         28 degrees C / 82 degrees F
      FPM Display            OK         31 degrees C / 87 degrees F
[...Output truncated...]
```

What It Means For M5, M10, M20, and M40 routers, the command output displays the craft interface state, which can be OK or Absent.

For M40e and M160 routers, the command output displays the FPM Chassis Management Bus (CMB) status and the FPM display status, which can be OK or Absent.

For M320 routers, the command output displays the FPM CMB status only.

For T320 routers and T640 routing nodes, the command output displays the FPM circuitry and the FPM display status, which can be OK or Absent.

Alternative Action (For M40e, M160, M320, and T320 routers and the T640 routing node) To monitor the craft interface environmental status, use the following CLI command:

user@host> **show chassis environment fpm**

```
user@host> show chassis environment fpm
FPM status:
  State                       Online
  FPM CMB Voltage:
    5.0 V bias           5030 mV
    8.0 V bias           8083 mV
  FPM Display Voltage:
    5.0 V bias           4998 mV
  FPM CMB temperature      34 degrees C / 93 degrees F
  FPM Display temperature  35 degrees C / 95 degrees F
  CMB Revision             12
```

The command output displays the status of the FPM or craft interface, which can be Online or Offline. It also displays information about the power supplied to the FPM CMB or FPM GBUS, information about the FPM display power supply, the temperature of the air flowing past the FPM CMB or FPM GBUS and the FPM display, and the CMB or GBUS revision level.

Viewing Craft Interface Information from the Command Line

If the craft interface fails, you can still display the craft interface information from the CLI. The values reflect what would be visible if the craft interface were operating normally.

Action To display craft interface information, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
WARNING: Front panel not present.  The following values
         reflect what would be currently visible.

Red alarm:     LED on, relay on
Yellow alarm:  LED on, relay on
Host OK LED:   On
Host fail LED: Off

FPCs     0  1  2  3
-------------------
Green    .  .  *  *
Red      .  .  .  .

LCD screen:
     +--------------------+
     |myrouter            |
     |2 Alarms active     |
     |R: fxp0: link down  |
     |Y: Bchip uCode ovflw|
     +--------------------+
```

What It Means

The command output displays the information that is currently displayed on the craft interface, including the alarm indicator status, the component status, and the alarm messages currently displayed on the LCD display. The command output is for an M20 router. A craft interface failure generates a red alarm, and you see an fpx0: link down alarm in the LCD screen output. The fpx0 interface or the Ethernet management interface provides an out-of-band method of connecting to the router from the craft interface.

Verifying Craft Interface Failure

When the craft interface fails, you might not see any lights on the craft interface panel and the LCD display will be blank. In addition, the buttons on the panel might not work as indicated.

On M5 and M10 routers, you can use the lamp test button to ensure that the alarm LED lights are working properly.

Steps To Take

To verify craft interface failure, follow these steps:

1. Display Craft Interface Alarms on page 206
2. Display Craft Interface Error Messages in the System Log File on page 207
3. Display Craft Interface Messages in the Chassis Daemon Log File on page 208
4. Display Craft Interface Hardware Information on page 208

Step 1: Display Craft Interface Alarms

A craft interface failure generates a red or yellow alarm, or both. For information about conditions that trigger craft interface alarms, see “Gather Component Alarm Information” on page 60.

Action To display a craft interface alarm, use the following CLI command:

user@host> **show chassis alarms**

Sample Output For an M20 router:

```
user@host> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2002-05-09 00:00:54 UTC  Major  fxp0: ethernet link down
```

For M40e and M160 routers:

```
user@host> show chassis alarms
2 alarms currently active
Alarm time               Class  Description
2002-06-07 18:20:00 UTC  Minor  Craft Failure
2002-06-07 18:20:00 UTC  Minor  Front Top Fan Absent
```

What It Means (M20 router) If the craft interface fails or is removed, you see an alarm. For example, if you remove the craft interface, a major management Ethernet interface down alarm is generated. The Ethernet link to the router is down. The Ethernet management interface, or fpx0, provides an out-of-band method for connecting to the router. You can connect to the management interface over the network using utilities such as secure shell (SSH) and telnet. The Simple Network Management Protocol (SNMP) can use the management interface to gather statistics from the router.

(M40e and M160 routers) The craft interface is connected to the front top fan assembly. If the craft interface fails or is removed, a craft interface failure alarm and a front top fan absence alarm are generated.

Step 2: Display Craft Interface Error Messages in the System Log File

Action To display craft interface error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output For an M20 router:

```
user@host> show log messages
Jun  3 16:43:19 flitter ssb CM(0): ALARM SET: (Major) fxp0: ethernet link down
Jun  3 16:43:19 flitter craftd[582]: forwarding display request to chassisd:
type = 4, subtype = 43
Jun  3 16:43:19 flitter alarmd[581]: Alarm set: fxp0 color=RED, class=ETHER,
reason=fxp0: ethernet link down
Jun  3 16:43:19 flitter mib2d[586]: SNMP_TRAP_LINK_DOWN: ifIndex 1,
ifAdminStatus up(1), ifOperStatus down(2), ifName fxp0
Jun  3 16:43:21 flitter /kernel: fxp0: media DOWN 100Mb / full-duplex
```

For M40e and M160 routers:

```
user@host> show log messages
Jun  7 18:18:50 myrouter craftd[2654]:  Minor alarm set, Front Top Fan Absent
Jun  7 18:18:50 myrouter chassisd[2652]: CHASSISD_BLOWERS_SPEED: blowers
being set to full speed [fan/blower missing]
Jun  7 18:18:50 myrouter alarmd[2653]: Alarm set: Fan color=YELLOW,
class=CHASSIS, reason=Front Top Fan Absent
Jun  7 18:18:50 myrouter craftd[2654]: fpm led error: Unknown error: -1
Jun  7 18:18:50 myrouter alarmd[2653]: Alarm set: Craft IF color=YELLOW,
class=CHASSIS, reason=Craft Failure
Jun  7 18:18:50 myrouter craftd[2654]:  Minor alarm set, Craft Failure
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Use the show log messages CLI command to browse error messages that are generated at least 5 minutes before and after an event. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events prior to the event.

For an M20 router, the messages file output shows that the Ethernet management interface (fpx0) that provides an out-of-band method for connecting to the router from the craft interface is down. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

For an M160 router, since the craft interface is attached to the front top fan, you see both craft interface and fan error messages.

Step 3: Display Craft Interface Messages in the Chassis Daemon Log File

The chassis daemon (chassisd) log file keeps track of the state of each chassis component.

Action To display craft interface status messages in the chassisd log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jun  7 18:18:50 *** inventory change ***
Jun  7 18:18:50 fru 42 set alarm 0x2
Jun  7 18:18:50 alarm op fru 42 op 1 reason 2
Jun  7 18:18:50 send: yellow alarm set, class 100 obj 100 reason 2
Jun  7 18:18:50 front top blower removed
Jun  7 18:18:50 FPM set alarm 0x1
Jun  7 18:18:50 alarm op fru 33 op 1 reason 1
Jun  7 18:18:50 send: yellow alarm set, class 100 obj 106 reason 106
Jun  7 18:18:50 FPM removed
Jun  7 18:18:50 CHASSISD_BLOWERS_SPEED: blowers being set to full speed
[fan/blower missing]
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Step 4: Display Craft Interface Hardware Information

Action To display the craft interface hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output For M5, M10, M20, and M40 routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
[...Output truncated...]
Display          REV 07   710-000150   AA7812
```

For M40e, M160, M320, and T320 routers and T640 routing nodes:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
[...Output truncated...]
FPM CMB          REV 03   710-001642   AH5159
FPM Display      REV 01   710-001647   AA2920
[...Output truncated...]
```

What It Means For M5, M10, M20, and M40 routers, the command output displays the display version level, part number, and serial number. For M40e, M160, M320, and T320 routers and T640 routing nodes, the command output displays the hardware information for the FPM CMB or the FPM GBUS and the FPM display. If the craft interface has failed or is absent, you will not see the craft interface or FPM hardware information in the command output.

Replacing the Craft Interface

The craft interface is hot-removable and hot-insertable. You can remove and replace it without powering down the router or disrupting routing functions.

NOTE: The M5 and M10 router craft interface is a part of the router chassis. You cannot remove it.

Steps To Take To replace the craft interface, do one of the following:

1. Replace the M20 Router Craft Interface on page 209
2. Replace the M40 Router Craft Interface on page 209
3. Replace the M40e and M160 Router Craft Interface on page 210
4. Replace the M320 Router Craft Interface on page 211
5. Replace the T320 Router and T640 Routing Node Craft Interface on page 212

Step 1: Replace the M20 Router Craft Interface

Action To remove the M20 router craft interface, follow these steps:

1. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
2. Unscrew the thumbscrews on the left and right sides of the card carrier to unseat the craft interface from the midplane.
3. Flip the ends of the two extractor clips, which are adjacent to the thumbscrews, toward the outside edges of the router.
4. Grasp both sides of the craft interface and slide it about three-quarters of the way out of the router.
5. Move one of your hands underneath the craft interface to support it, and slide the craft interface completely out of the chassis.

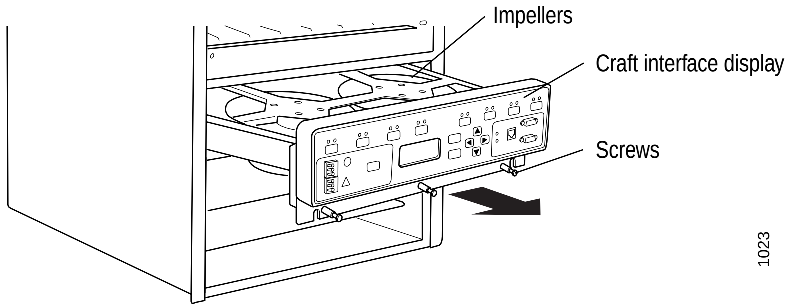
Step 2: Replace the M40 Router Craft Interface

The craft interface is attached to the lower impeller tray.

Action To remove the M40 router craft interface, follow these steps:

1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
2. Unscrew the three screws at the bottom edge of the lower impeller tray.
3. Grasp the sides of the lower impeller tray and slide it out of the chassis. (See Figure 77 on page 210.)

Figure 77: Removing the Lower Impeller Tray



Step 3: Replace the M40e and M160 Router Craft Interface

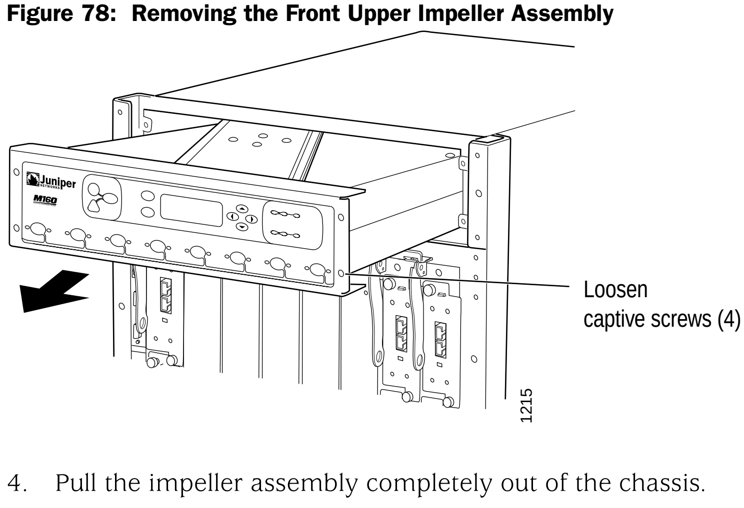
The craft interface is attached to the upper impeller assembly (front top blower).

Action To remove the M40e and M160 router craft interface, follow these steps:

1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
2. Unscrew the captive screws at the corners of the impeller assembly (the craft interface).
3. Grasp the impeller assembly and pull it halfway out of the chassis. (See Figure 78.)

CAUTION: If the impeller is still spinning, do not put your fingers or any tool into the impeller assembly as you pull it out. To avoid injury, wait until the impeller stops spinning before removing the assembly.

Figure 78: Removing the Front Upper Impeller Assembly



4. Pull the impeller assembly completely out of the chassis.
5. Place the assembly top-side down (the lettering on the craft interface is upside down) on an antistatic mat on a flat, stable surface.

6. Using a Phillips screwdriver, loosen and remove the four screws that secure the bottom of the craft interface housing to the impeller assembly.

7. Turn the impeller assembly over so that the lettering on the craft interface is right side up.

8. Using a Phillips screwdriver, loosen and remove the four screws that secure the top of the craft interface housing to the impeller assembly.

9. Using a Phillips screwdriver, loosen and remove the screws located on the rear side of the craft interface at the side. There are two screws at each side, located near the holes for the captive screws that secure the impeller assembly to the chassis.

10. Grasp the sides of the craft interface and pull it straight off the front of the impeller assembly.

Step 4: Replace the M320 Router Craft Interface

The craft interface is located on the front of the chassis above the FPC card cage.

Action To remove the craft interface, follow these steps:

NOTE: Removing the front upper fan tray before you remove the craft interface might make it easier to grasp the craft interface as you remove it. For instructions on removing a front fan tray, see the appropriate router hardware guide.

---

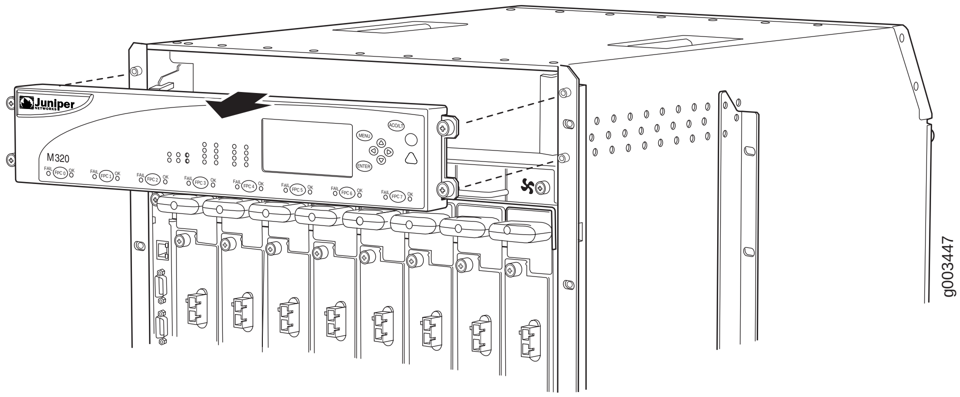
1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis.

2. Remove the upper cable guards by loosening the three captive screws on each cable guard.

3. Completely loosen the four captive screws that attach the craft interface to the chassis.

4. Grasp the craft interface by the left and right flanges and carefully pull it straight out of the chassis. (See Figure 75 on page 201.)

Figure 79: Remove the Craft Interface



Step 5: Replace the T320 Router and T640 Routing Node Craft Interface

The craft interface is located on the front of the chassis above the FPC card cage.

Action To remove the craft interface, follow these steps:

NOTE: Removing the front upper fan tray before you remove the craft interface might make it easier to grasp the craft interface as you remove it. For instructions on removing a front fan tray, see the appropriate nrouter hardware guide.

---

1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis.
2. Completely loosen the screws at the four corners of the craft interface.
3. Insert the blade of a flat-blade screwdriver into the slot on one side of the craft interface, then gently pry that side out from the chassis.
4. Repeat Step 3 for the other side of the craft interface.
5. Grasp the craft interface by the top and bottom edges and carefully pull it straight out of the chassis.

Locating the Craft Interface Serial Number ID Label

If the craft interface has failed or is absent, it does not appear in the hardware list output when you use the show chassis hardware command. You must remove the craft interface and manually locate the craft interface serial number ID label.

NOTE: The M5 and M10 router craft interfaces are part of the chassis. You cannot remove them.

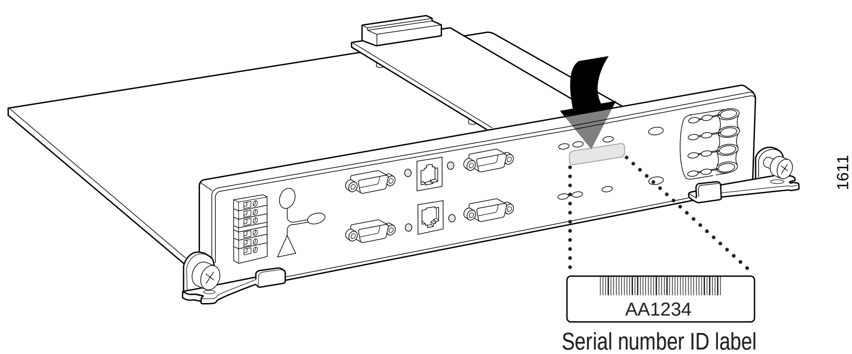
Steps To Take To locate the craft interface serial number ID label, do one of the following:

1. Locate the M20 Router Craft Interface Serial Number ID Label on page 213
2. Locate the M40 Router Craft Interface Serial Number ID Label on page 214
3. Locate the M40e and M160 Router Craft Interface Serial Number ID Label on page 214
4. Locate the M320 Router Craft Interface Serial Number ID Label on page 215
5. Locate the T320 Router and T640 Routing Node Craft Interface Serial Number ID Label on page 215

Step 1: Locate the M20 Router Craft Interface Serial Number ID Label

Action To locate the M20 router craft interface serial number ID label, look on the back of the craft interface panel (see Figure 80).

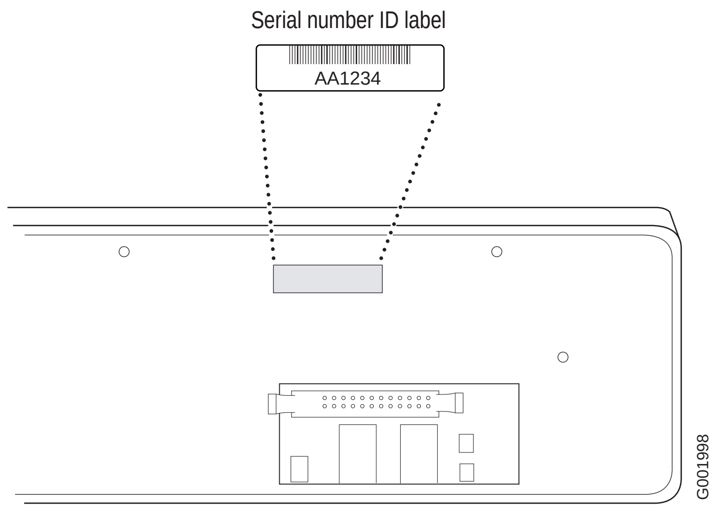
Figure 80: M20 Router Craft Interface Serial Number ID Label



Step 2: Locate the M40 Router Craft Interface Serial Number ID Label

Action To locate the M40 router craft interface serial number ID label, look on the back of the panel, above the connector (see Figure 81).

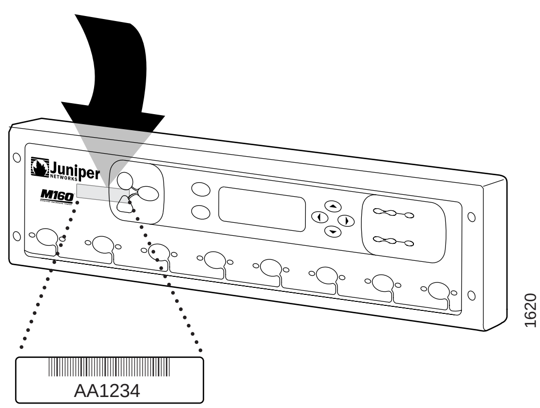
Figure 81: M40 Router Craft Interface Serial Number ID Label



Step 3: Locate the M40e and M160 Router Craft Interface Serial Number ID Label

Action To locate the M40e and M160 router serial number ID label, look on the back of the panel, behind the alarm LEDs (see Figure 82).

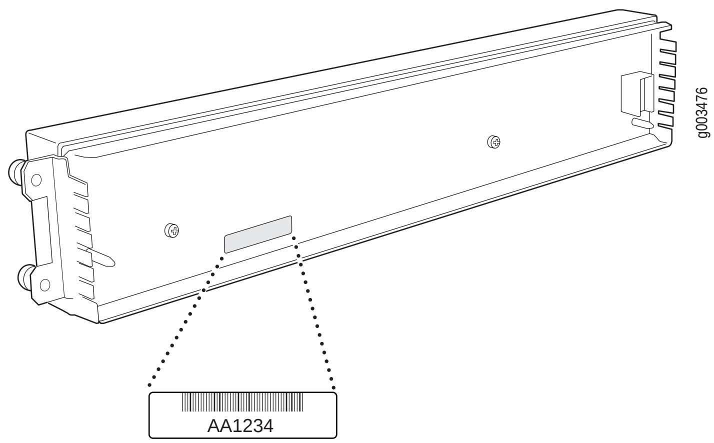
Figure 82: M40e and M160 Router Craft Interface Serial Number ID Label



Step 4: Locate the M320 Router Craft Interface Serial Number ID Label

Action To locate the M320 router serial number, look on the back of the craft interface panel, behind the alarm LEDs (see Figure 83).

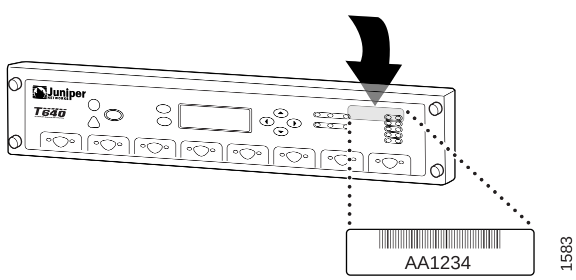
Figure 83: M320 Router Serial Number ID Label



Step 5: Locate the T320 Router and T640 Routing Node Craft Interface Serial Number ID Label

Action To locate the T320 router and T640 routing node serial number, look on the back of the craft interface panel, behind the alarm LEDs (see Figure 84).

Figure 84: T320 Router and T640 Routing Node Serial Number ID Label



Returning the Craft Interface

The craft interface is hot-removable and hot-insertable. You can remove or replace a craft interface without powering down the system and disrupting routing functions.

Action To return the craft interface, see "Replacing a Failed Component" on page 122 or the appropriate router hardware guide.

Chapter 18

Monitoring Power Supplies

You monitor and maintain the power supplies to ensure that power is distributed to the router components. (See Table 53.)

Table 53: Checklist for Monitoring Power Supplies

Monitor Power Supply Tasks	Command or Action
Understanding Power Supplies on page 218	
■ M5/M10 Router Power Supplies on page 219 ■ M7i Router Power Supplies on page 220 ■ M10i Router Power Supplies on page 221 ■ M20 Router Power Supplies on page 222 ■ M40 Router Power Supplies on page 223 ■ M40e Router Power Supplies on page 224 ■ M160 Router Power Supplies on page 226 ■ M320 Router Power Supplies on page 227 ■ T320 Router Power Supplies on page 228 ■ T640 Routing Node Power Supplies on page 229	
Checking the Power Supply Cables on page 229	Check the power supply cables.
Checking the Power Supply Status on page 230	
1. Check the Power Supply Environmental Status on page 230	show chassis environment (M40e, M160, and T320 router and T640 routing node only) show chassis environment pem *slot*
2. Check the Power Supply LEDs on page 232	Check the LEDs on the power supply faceplate.
Checking for Power Supply Alarms on page 235	
1. Display Current Power Supply Alarms on page 235	show chassis alarms
2. Display Power Supply Error Messages in the System Log File on page 238	show log messages | match “power supply”
3. Display Power Supply Error Messages in the Chassis Daemon Log File on page 238	show log chassisd | match pem
Verifying Power Supply Failure on page 239	
1. Check the Power Supply Power Switch on page 239	Check the power supply power switch.
2. Check the Circuit Breaker on page 239	Make sure that the power switch is on.
3. Perform a Power Supply Swap Test on page 240	Replace the faulty power supply with one that works.
4. Check the Router Cooling System on page 240	show chassis environment

Monitor Power Supply Tasks	Command or Action
5. Test the Power Supply on page 241	Press the power supply self-test button.
Getting Power Supply Hardware Information on page 241	
1. Display the Power Supply Hardware Information on page 242	show chassis hardware
2. Locate the Power Supply Serial Number ID Label on page 242	Look on the power supply faceplate or look on the back of the power supply.
Replacing the Power Supplies on page 250	(M5, M10, M20, and M40 routers) Turn off the power to the individual power supply before removing it from the chassis. (M40e, M160, and T320 routers and T640 routing node) Switch the corresponding circuit breaker off before removing the power supply. Follow the procedure in the appropriate router hardware guide.

Understanding Power Supplies

Purpose Inspect the power supplies to ensure that they distribute power to the other router components according to their voltage requirements.

What Is a Power Supply The power supplies are internally connected to the midplane, which delivers the power input from the circuit breaker box and distributes the different output voltages produced by the power supplies to the router's components, depending on their voltage requirements.

Table 54 lists some router characteristics for each router type.

Table 54: Router Power Supply Characteristics

Power Supply Characteristic	M5/ M10	M7i/ M10i	M20	M40	M40e	M160	M320	T320	T640
Watts per AC/DC power supply	434 W	293 W	750 W	1500 W	AC 2900 W DC 3000 W	DC original 2600 W DC enhanced 3200 W	1750 W	3200 W	6500 W
Supports both AC and DC power supplies	Yes	Yes	Yes	Yes	Yes	No; original or enhanced DC only	Yes	No; DC only	No; DC only
Turn off power supply before removing	X	X	X	X					
Turn off circuit breaker before removing power supply					X	X	X	X	X

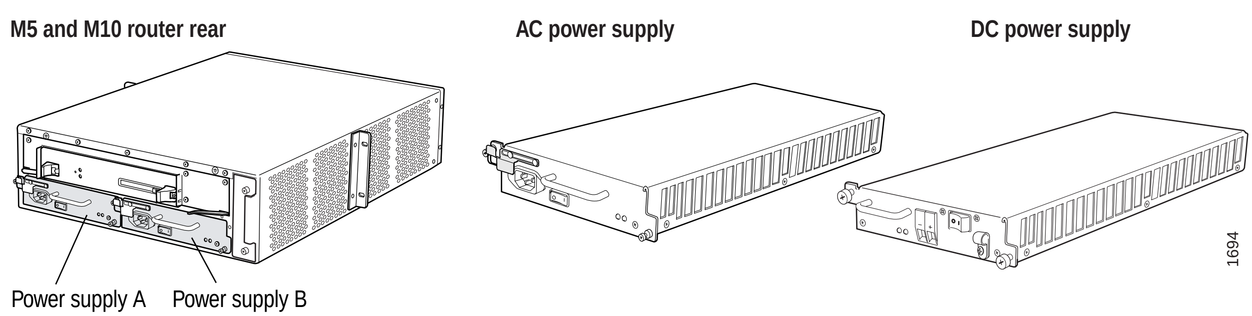
Power supplies in the router must be of the same type: either two AC or two DC power supplies. You cannot mix power supply types. The M160 router supports DC power supplies only.

The following sections describe each routing platform power supply location and type:

M5/M10 Router Power Supplies

Two load-sharing, isolated power supplies are located at the bottom rear of the M5 and M10 router chassis. The routers use either AC or DC power. Figure 85 shows the M5 and M10 router power supplies and where they are installed in the chassis.

Figure 85: M5 and M10 Router Power Supplies



When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supply instantly begins providing all the power the router needs for normal functioning and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported. The two power supplies must be either both AC or both DC.

When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

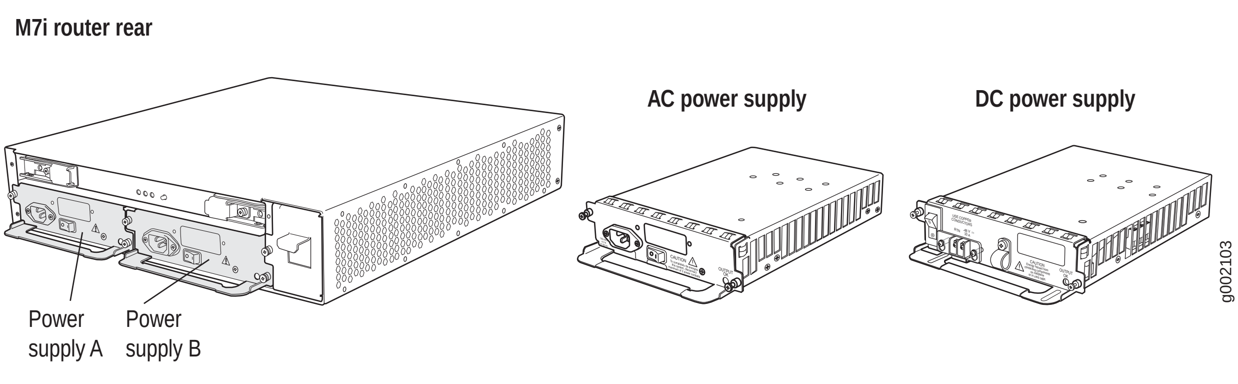
M7i Router Power Supplies

Two load-sharing, isolated power supplies are located at the bottom rear of the M7i router chassis. The router uses either AC or DC power. Figure 86 shows the M7i router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load.

For full redundancy, two power supplies are required. If a power supply stops functioning for any reason, the second power supply instantly begins providing all the power the router needs for normal functioning. The second power supply can provide full power indefinitely.

Figure 86: M7i Router Power Supplies



NOTE: When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

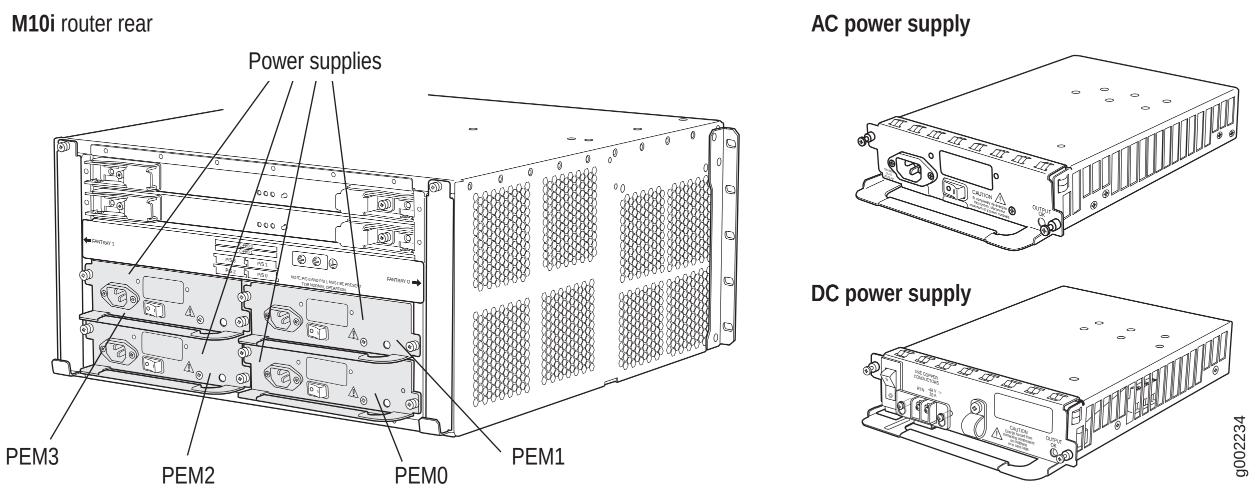
M10i Router Power Supplies

The M10i router uses either AC or DC power. You can install up to four load-sharing power supplies at the bottom rear of the chassis. Figure 87 shows the M10i router power supplies and where they are installed in the chassis.

The AC power supplies are fully redundant. If one power supply fails or is removed, the remaining power supplies instantly assume the entire electrical load. Two power supplies can provide full power for as long as the router is operational. Three power supplies are required for redundancy. Power supplies must be present in slots P/S 0 and P/S 1 for the router to operate.

The DC power supplies are fully redundant. The DC power supplies in slots P/S 0 and P/S 1 can provide full power to the router. Likewise, the DC power supplies in slots P/S 2 and P/S 3 can also provide full power. The DC power supplies in slots P/S 2 and P/S 3 jointly serve as the backup to the DC power supplies in slots P/S 0 and P/S 1. Power supplies must be present in slots P/S 0 and P/S 1 for the router to operate.

Figure 87: M10i Router Power Supplies



NOTE: AC and DC power supplies are required in slots P/S 0 and P/S 1 for the router to operate.

The DC power supplies in slots P/S 0 and P/S 1 must be powered by dedicated power feeds derived from feed A, and the DC power supplies in slots P/S 2 and P/S 3 must be powered by dedicated power feeds derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

M20 Router Power Supplies

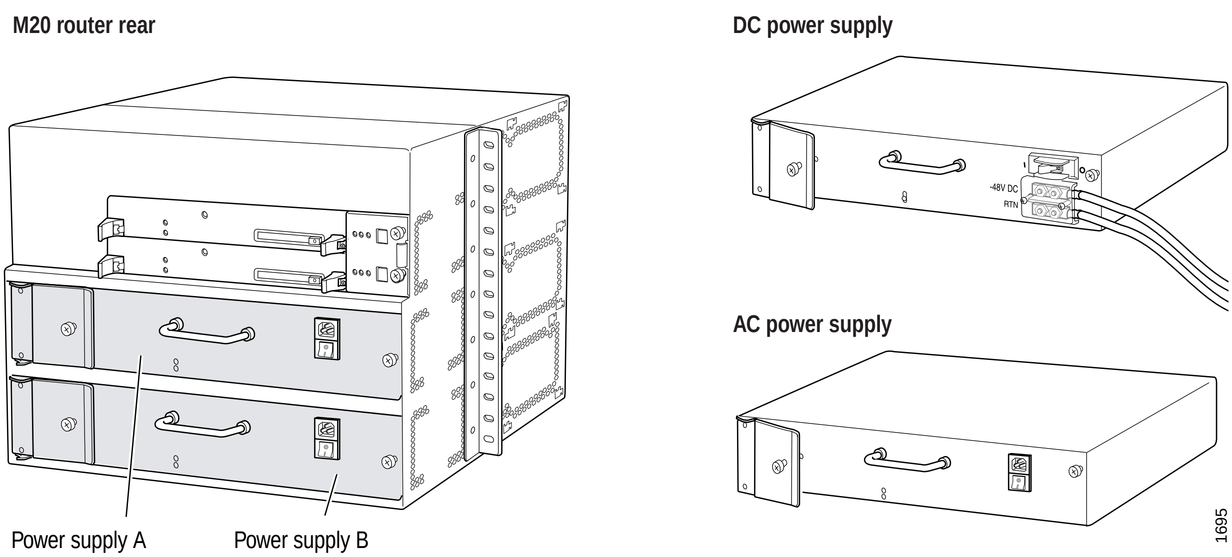
Two load-sharing, isolated power supplies are located at the bottom rear of the M20 router chassis.The router uses either AC or DC power. Figure 88 shows the M20 router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported. The two power supplies must be either both AC or both DC.

When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers and on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

Figure 88: M20 Router Power Supplies

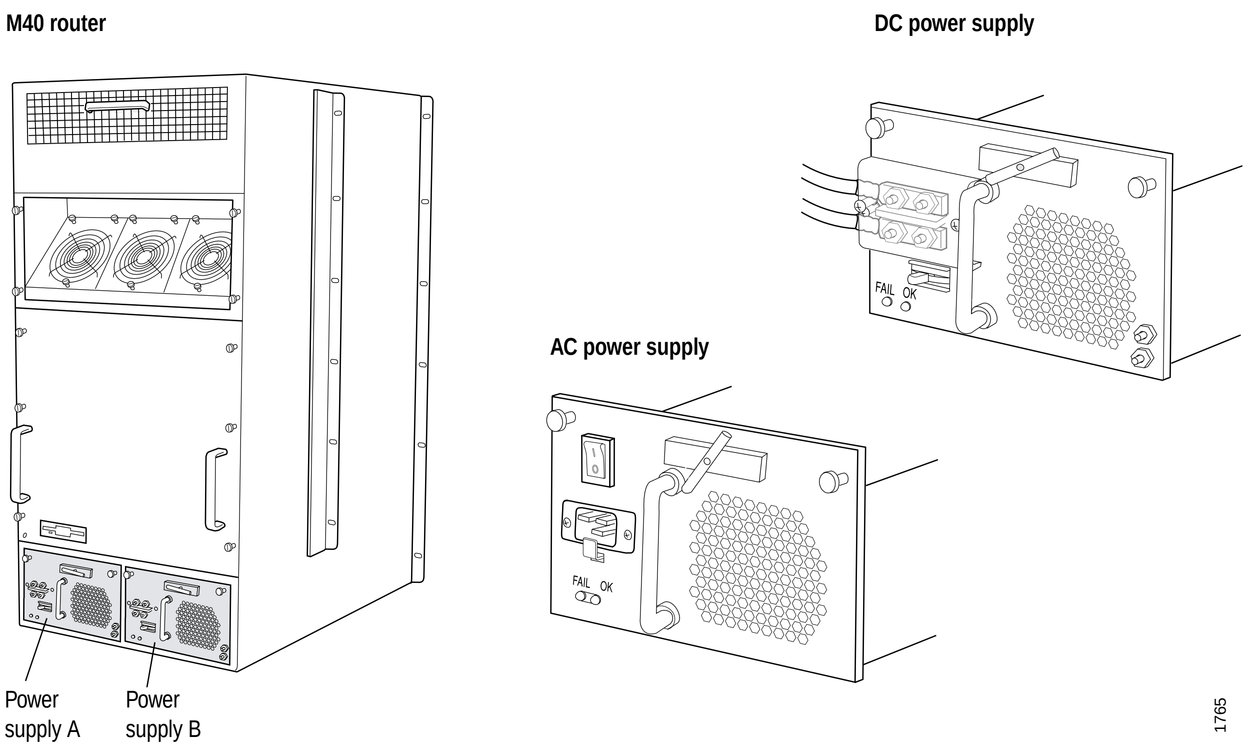


M40 Router Power Supplies

The M40 router can use either AC or DC power. Two load-sharing power supplies install into the bays located at the bottom rear of the chassis. As viewed from the rear of the chassis, the supply on the left is referred to as supply A and the supply on the right as supply B. Figure 89 shows the M40 router power supplies and where they are installed in the chassis.

The power supplies are fully redundant. When both power supplies are operational, they automatically share the electrical load. If one power supply stops functioning for any reason, the remaining power supply instantly begins providing all the power the router needs for normal functioning, and can provide full power indefinitely.

Figure 89: M40 Router Power Supplies



M40e Router Power Supplies

The M40e router uses either AC or DC power. Two load-sharing, pass-through power supplies are located at the bottom rear of the chassis. Figure 90 shows the M40e router power supplies and where they are installed in the chassis.

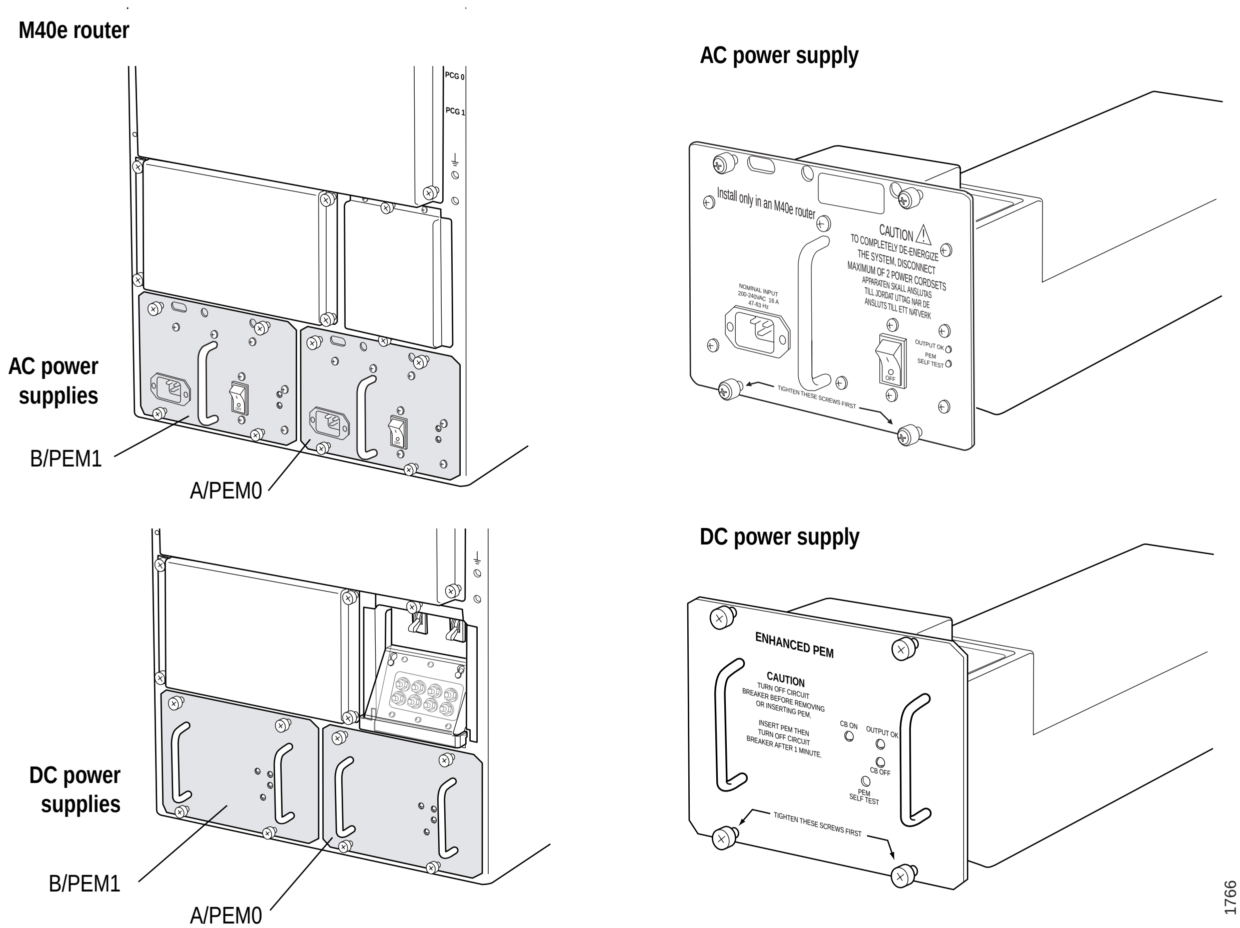
When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported and prevents the router from booting. If two power supplies are installed, they must be either both AC or both DC.

- A circuit breaker box must be installed on a DC-powered router, while a circuit breaker is incorporated into each AC power supply. Converting the router from AC to DC power or vice versa involves removing or installing the circuit breaker box. Only authorized service personnel should perform the conversion; this manual does not include instructions.

- When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

Figure 90: M40e Router Power Supplies

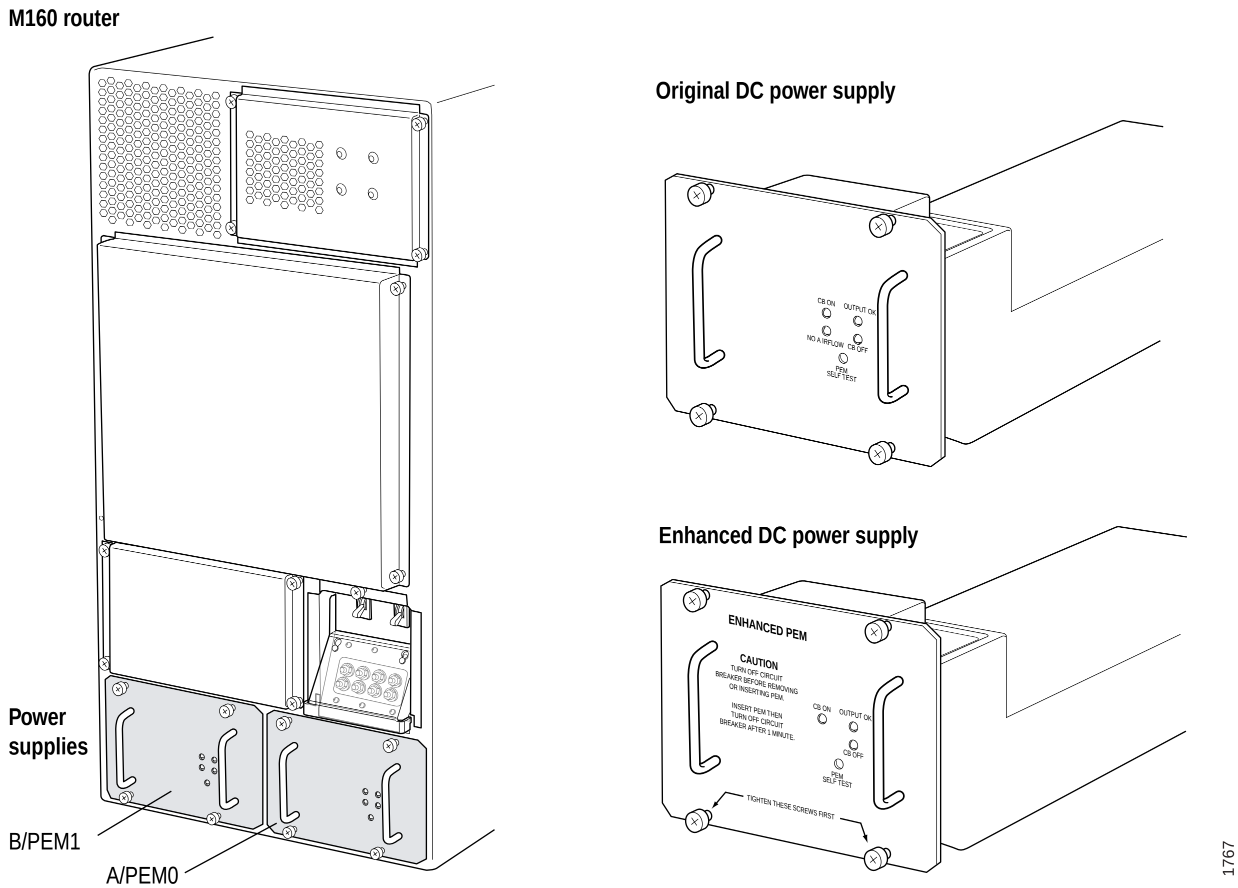


M160 Router Power Supplies

The M160 router uses DC power. Two load-sharing, pass-through power supplies are located at the bottom rear of the chassis. Figure 91 shows the M160 router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

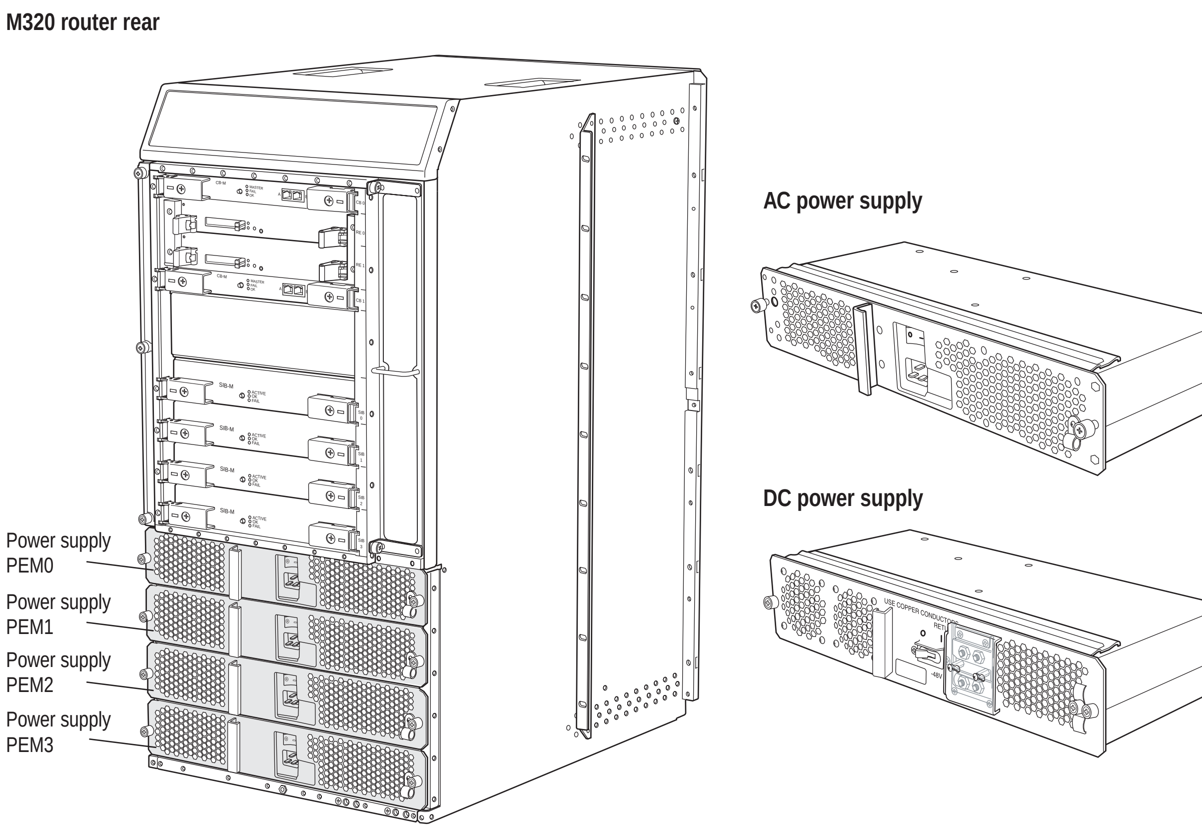
Figure 91: M160 Router Power Supplies



M320 Router Power Supplies

The M320 router uses either AC or DC power. Figure 92 shows the M320 router power supplies and where they are installed in the chassis.

Figure 92: M320 Router Power Supplies



The M320 router supports four power supplies. The AC power supplies are fully redundant. If one power supply fails or is removed, the remaining power supplies instantly assume the entire electrical load. Three power supplies can provide full power for as long as the router is operational.

In the M320 router DC power supply configuration, the router has four DC power supplies, located at the lower rear of the chassis in slots PEM0 through PEM3 (top to bottom). The DC power supplies in slots PEM0 and PEM2 are load-sharing and provide power to the Flexible PIC Concentrators (FPCs) in slots FPC3 through FPC7. The DC power supplies in slots PEM1 and PEM3 are load-sharing and provide power to the FPCs in slots FPC0 through FPC2, Switch Interface Boards (SIBs), Control Boards, and Routing Engines. All DC power supplies provide power to the fan trays.

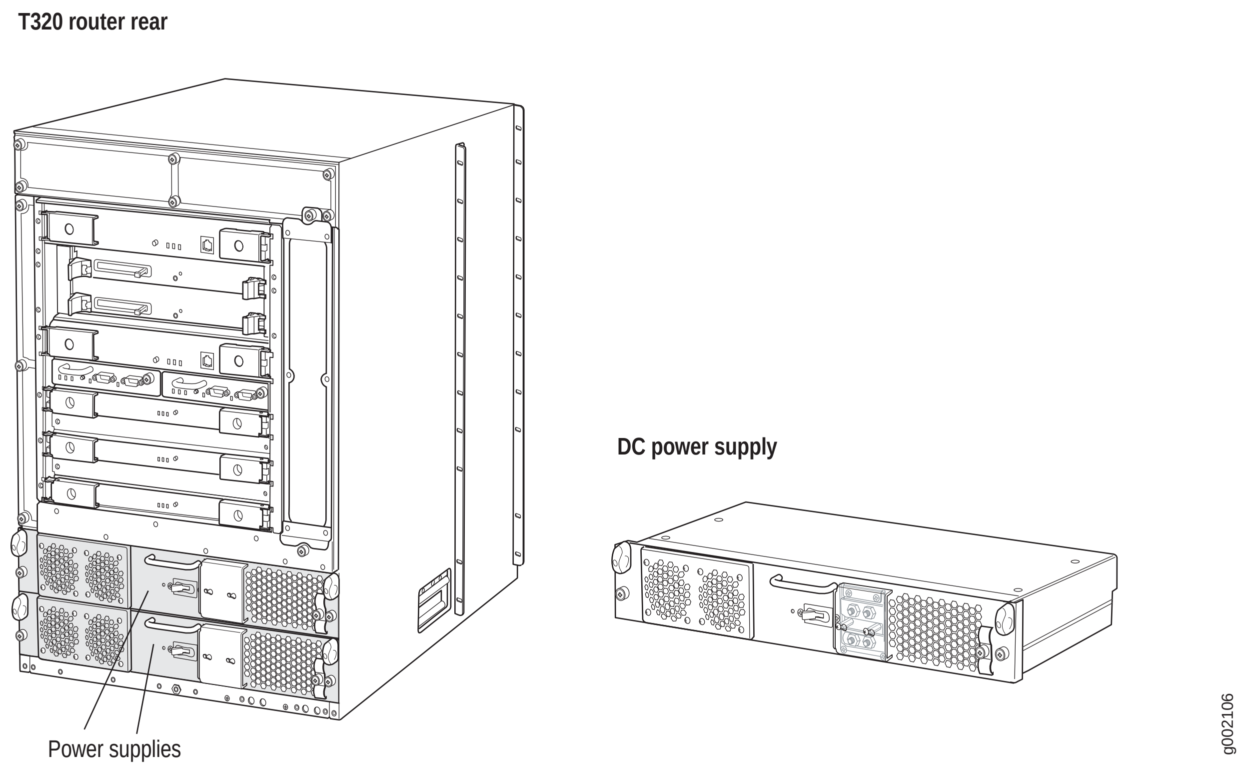
NOTE: The DC power supplies in slots PEM0 and PEM1 must be powered by dedicated power feeds derived from feed A, and the DC power supplies in slots PEM2 and PEM3 must be powered by dedicated power feeds derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated 15 A (250 VAC) circuit breaker.

T320 Router Power Supplies

Figure 93 shows the T320 router power supplies and where they are installed in the chassis.

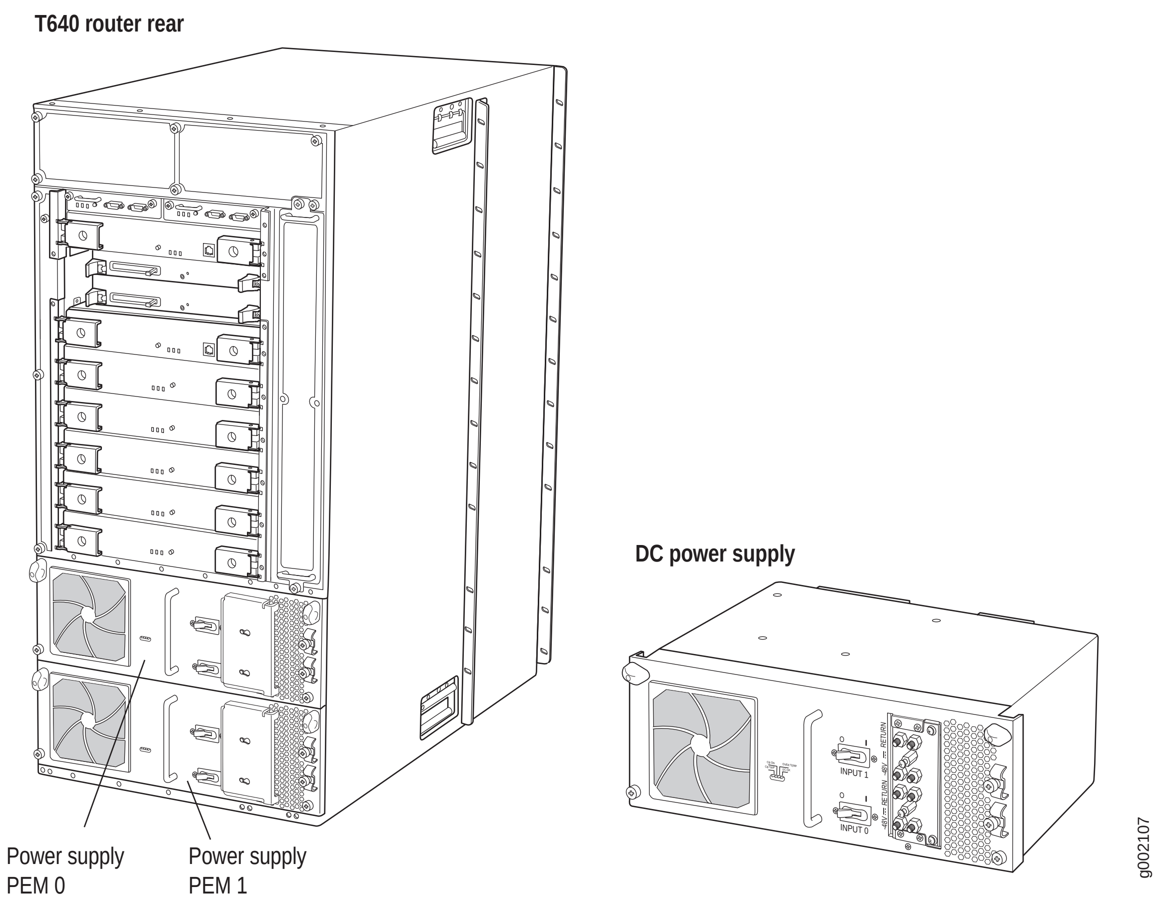
Figure 93: T320 Router Power Supplies Location



T640 Routing Node Power Supplies

Figure 94 shows the T640 routing node power supplies and where they are installed in the chassis.

Figure 94: T640 Routing Node Power Supplies



See Also
- Monitoring Redundant Power Supplies on page 507

Checking the Power Supply Cables

Action To check the power supply cables, follow these steps:

1. Verify that the power cable or power cord from the power source to the router is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable.

2. Make sure that the power and ground cables on each DC power supply are arranged so that they do not obstruct access to the other power supply or to the Routing Engine.

3. Periodically inspect the site to ensure that the cables connected to the power supply are securely in place and are properly insulated.

Checking the Power Supply Status

Steps To Take To check the power supply status, follow these steps:

1. Check the Power Supply Environmental Status on page 230
2. Check the Power Supply LEDs on page 232

Step 1: Check the Power Supply Environmental Status

Action To check the power supply environmental status, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis environment**

Sample Output For M5, M10, M20, and M40 routers:

```
user@host> show chassis environment
Class Item                 Status     Measurement
Power Power Supply A       OK
      Power Supply B       Absent
[...Output truncated...]
```

For M7i and M10i routers:

```
user@host> show chassis environment
Class Item                 Status     Measurement
Power Power Supply 0       OK
      Power Supply 1       Absent
[...Output truncated...]
```

For M40e, M160, M320 and T320 routers and T640 routing nodes:

```
user@host> show chassis environment
Class Item                 Status     Measurement
Power PEM 0                OK
      PEM 1                OK
[...Output truncated...]
```

What It Means The command output displays the status of both power supplies installed in the router.

For M5, M10, M7i, M10i, M20, and M40 routers, the command output displays the power supply slot number and status. The status can be OK, Testing (during initial power-on), Failed, or Absent. A Failed condition triggers the red alarm LED on the craft interface.

For M40e, M160, M320, and T320 routers and T640 routing nodes, the output displays the power supply slot number and status for the Power Entry Modules (PEMs). The status can be OK, Absent, or Check.

Alternative Action For the M40e, M160, M320, and T320 routers and the T640 routing node, to display the power supply status, use the following CLI command:

user@host> **show chassis environment pem**

```
user@host> show chassis environment pem
PEM 0 status:
  State                         Online
  Temperature                   OK
  DC input                      OK
  DC output                     OK
  Load                          Less than 20 percent
  Voltage:
    48.0 V input        69028 mV
    48.0 V fan supply   48839 mV
    5.0 V bias           5013 mV
    8.0 V bias           8253 mV
PEM 1 status:
  State                         Online
  Temperature                   OK
  DC input                      OK
  DC output                     OK
  Load                          Less than 20 percent
  Voltage:
    48.0 V input        69307 mV
    48.0 V fan supply   49170 mV
    5.0 V bias           4991 mV
    8.0 V bias           8263 mV
```

For each PEM, the command output displays the slot number, status, temperature, DC input and output, load percentage, and voltage. You can display the status of a particular power supply by specifying the *slot* number.

For T320 routers and T640 routing nodes, the command output displays the PEM slot number, status, temperature, DC input status, and DC output for each Flexible PIC Concentrator (FPC), SONET Clock Generator (SCG), Control Board, and Switch Interface Board (SIB). You can display the status of a particular power supply by specifying the *slot* number.

```
user@host> show chassis environment pem
PEM 1 status:
  State                             Online
  Temperature                    33 degrees C / 91 degrees F
  DC input:                         OK
  DC Output:            Voltage   Current        Power    Load
       FPC 0              53783      3368          181      24
       FPC 1                  0         0            0       0
       FPC 2                  0         0            0       0
       FPC 3                  0         0            0       0
       FPC 4              54041      3462          187      24
       FPC 5              53883      5187          279      37
       FPC 6                  0         0            0       0
       FPC 7                  0         0            0       0
  SCG/CB/SIB              54066      4031          217      18
```

Step 2: Check the Power Supply LEDs

Action To check the power supply status, look at the four LEDs on the faceplate. Table 55 describes the M5 and M10 router output LED and self-test button for both the AC and DC power supplies.

Table 55: M5 and M10 Router Power Supply LED and Self-Test Button

Label	Color	State	Description
OUTPUT OK	Blue	On steadily	Power supply is functioning normally, input is occurring, outputs are within range, and the temperature is within range.
		Blinking	Power supply has failed.
SELF-TEST	(button)	–	Power supply is in self-test mode.

Table 56 describes the functions of the LED on both the M7i and M10 router AC and DC power supplies.

Table 56: M7i and M10i Router AC/DC Power Supply LED

Label	Color	State	Description
OUTPUT OK	Green	On steadily	Power supply is inserted and is functioning normally, input is occurring, outputs are within range, and the temperature is within range.
		Blinking	Power supply is not functioning, is starting up, or is not properly inserted, or airflow is not sufficient.

Table 57 describes the functions of the M20 router power supply LEDs.

Table 57: M20 Router Power Supply LEDs

Label	Color	State	Description
OK	Green	On steadily	Power supply is functioning normally, input is occurring, outputs are within range, temperature is within range, and fans are operational.
FAIL	Amber	On steadily	Power supply has failed.

Table 58 describes the functions of the M40 router power supply LEDs.

Table 58: M40 Router Power Supply LEDs

Label	Color	State	Description
OK	Green	On steadily	Power supply is functioning normally, input is occurring, outputs are within range, temperature is within range, and fans are operational.
FAIL	Red	On steadily	Power supply has failed.

Table 59 describes the functions of the M40e router AC power supply LED.

Table 59: M40e Router AC Power Supply LED

Label	Color	State	Description
OUTPUT OK	Green	On steadily	Power supply is inserted and is functioning normally.
		Blinking slowly	Power supply is not plugged in, or power switch is in the off position (when other AC power supply is functioning).
		Blinking rapidly	Power supply is starting up.

Table 60 describes the functions of the M40e router DC power supply LEDs.

Table 60: M40e Router DC Power Supply LEDs

Label	Color	State	Description
CB ON	Green	On steadily	Power supply is inserted correctly and is receiving power. Circuit breaker is on.
OUTPUT OK	Blue	On steadily	Power supply is inserted and is functioning normally.
		Blinking	Power supply is not functioning, is starting up, is not properly inserted, or airflow is not sufficient.
CB OFF	Amber	On steadily	Power supply is functioning, but the circuit breaker is off.

Table 61 describes the functions of the M160 router DC power supply LEDs.

Table 61: M160 Router Power Supply LEDs

LED	Color	State	Description
CB ON	Green	On steadily	Power supply is inserted correctly and is receiving power. Circuit breaker is on.
OUTPUT OK	Blue	On steadily	Power supply is inserted and is functioning normally.
		Blinking	Power supply is not functioning, is going through startup, is not properly inserted, or airflow is not sufficient.
		Off	Power supply is not functioning.
NO AIRFLOW (Original power supply only)	Amber	On steadily	Power supply is inserted, but airflow around the power supply is not sufficient.
CB OFF	Amber	On steadily	Power supply is functioning, but the circuit breaker is off.

Table 62 describes the functions of the M320 router AC and DC power supply LED.

Table 62: M320 Router AC/DC Power Supply LED

Label	Color	State	Description
OUTPUT OK	Blue	Off	No power applied to power supply.
		Blinking	■ Power supply blinks for 5 seconds after initial power on. ■ Power supply is installed, but not powered on, and is receiving bias power from a proword on power supply. ■ Input voltage is invalid ■ Power supply has failed.
		On steadily	Power supply is functioning normally.

Table 63 describes the functions of the M320 router AC and DC power supply LED.

Table 63: T320 Router DC Power Supply LED

Label	Color	State	Description
DC OK	Blue	On steadily	Power supply is installed correctly and is functioning normally.
		Blinking	Power supply is starting up, is not functioning, or is not properly installed.

Table 64 describes the functions of the T640 routing node DC power supply LEDs.

Table 64: T640 Routing Node Power Supply LEDs

LED	Color	State	Description
CB ON	Green	On steadily	Power supply is installed correctly and is functioning normally, is receiving power, and the circuit breaker is on.
CB TRIP	Amber	On steadily	Circuit breaker not turned on, or host subsystem has detected a failure and has turned the circuit breaker off.
OVER TEMP	Amber	On steadily	Power supply has exceeded the recommended temperature.
DC OK	Blue	On steadily	Power supply is installed correctly and is functioning normally.
		Blinking	Power supply is starting up, is not functioning, or is not properly installed.

Alternative Actions For M40e and M160 routers, if all LEDs are off on both power supplies, either someone has switched off power to the router or the system temperature has exceeded the acceptable maximum. The host module shuts down both power supplies. There is no power to the router, so the alarm LEDs on the craft interface are not lit and the LCD display is blank.

Excessive system temperature is almost always caused by excessive environmental temperature. Correct the environmental temperature before repowering the router.

If all LEDs on one power supply are off, but the LEDs on the other supply indicate that it is functioning properly, or the LEDs on both power supplies indicate a problem, do the following:

1. Check the current alarms by using the show chassis alarms CLI command or by looking at the router craft interface.
2. Check that the power switch is in the ON (|) position (on the circuit breaker box for a DC-powered router, or on the power supply faceplate for an AC-powered router).
3. Perform a swap test on the power supplies (see “Perform a Power Supply Swap Test” on page 240).

Checking for Power Supply Alarms

For a listing of power supply alarm conditions, remedy, and alarm severity by routing platform type, see “Display the Current Router Alarms” on page 61.

Steps To Take To check for power supply alarms, follow these steps:

1. Display Current Power Supply Alarms on page 235
2. Display Power Supply Error Messages in the System Log File on page 238

Step 1: Display Current Power Supply Alarms

Action To display power supply alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
4 alarms currently active
Alarm time               Class  Description
2002-04-08 15:25:12 PDT  Major  Power Supply A 2.5 volt output failed
2002-04-08 15:25:12 PDT  Major  Power Supply A 5 volt output failed
2002-04-08 15:25:12 PDT  Major  Power Supply A 3.3 volt output failed
2002-04-08 15:25:12 PDT  Major  Power Supply A fan failed
```

What It Means The command output displays the alarm date, time, severity level, and description. Table 65 shows the power supply alarm descriptions that you see on the craft interface LCD and the alarms that you see at the CLI. For information about conditions that trigger power supply alarms, see "Gather Component Alarm Information" on page 60.

Table 65: Power Supply Alarms

Power Supplies	Craft Interface LCD Short Version	CLI Long Version
M5 and M10	N/A	Power supply *x* not providing power
M7i and M10i	N/A	Power supply *x* not providing power
M20	N/A	Power supply *x* not providing power
	N/A	Power supply *x* 3.3V failed
	N/A	Power supply *x* 5V failed
	N/A	Power supply *x* 2.5V failed
M40	Supply *x* FAIL	Power supply *x* not providing power
	Supply *x* 3V FAIL	Power supply *x* 3.3V failed
	Supply *x* 5V FAIL	Power supply *x* 5V failed
	Supply *x* 2V FAIL	Power supply *x* 2.5V failed
M40e	PEM *pem-ID* Removed	YELLOW ALARM - PEM *pem-ID* Removed
	PEM *pem-ID* High Temp	RED ALARM - PEM *pem-ID* High Temperature
	PEM *pem-ID* Output Fail	RED ALARM - PEM *pem-ID* Output Failure
	PEM *pem-ID* Input Fail	RED ALARM - PEM *pem-ID* Input Failure
M160	PEM *pem-number* Removed	YELLOW ALARM - PEM *pem-number* Removed
	PEM *pem-number* High Temp	RED ALARM - PEM *pem-number* High Temperature
	PEM *pem-number* Output Fail	RED ALARM - PEM *pem-number* Output Failure
	PEM *pem-number* Input Fail	RED ALARM - PEM *pem-number* Input Failure

Power Supplies	Craft Interface LCD Short Version	CLI Long Version
T320	PEM *pem-number* Removed	YELLOW ALARM - PEM *pem-number* Removed
	PEM *pem-number* Over Temp	RED ALARM - PEM *pem-number* Over Temperature
	PEM *pem-number* Output Fail	RED ALARM - PEM *pem-number* Output Failure
	PEM *pem-number* Input Fail	RED ALARM - PEM *pem-number* Input Failure
T640	PEM *pem-number* Removed	YELLOW ALARM—PEM *pem-number* Removed
	PEM *pem-number* Over Temp	RED ALARM—PEM *pem-number* Over Temperature
	PEM *pem-number* Output Fail	RED ALARM—PEM *pem-number* Output Failure
	PEM *pem-number* Input Fail	RED ALARM—PEM *pem-number* Input Failure

For information about what conditions trigger power supply alarms and their remedy for each router type, see “Display the Current Router Alarms” on page 61.

Alternative Action To display current power supply alarms and the alarm indicator states, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
Red alarm:     LED on, relay on
Yellow alarm:  LED off, relay off
Host OK LED:   On
Host fail LED: Off

FPCs     0  1  2  3
-------------------
Green    *  *  *  *
Red      .  .  .  .

LCD screen:
     +--------------------+
     |myrouter            |
     |4 Alarms active     |
     |R: Supply A 2v FAIL |
     |R: Supply A 5v FAIL |
     +--------------------+
```

What It Means The command output displays the alarm indicator status and the alarms that display on the craft interface LCD display.

(For M7i router) Check the red and yellow alarm LEDs on the FIC. Power supply failure or removal triggers an alarm that causes one or both of the LEDs to light.

Step 2: Display Power Supply Error Messages in the System Log File

Action To display power supply error messages that are generated in the system log file, use the following CLI command:

user@host> **show log messages | match "power supply"**

Sample Output

```
user@host> show log messages | match "power supply"
Apr  8 14:00:15 myrouter scb CM: ALARM SET: (Major) Power Supply A fan failed
Apr  8 14:00:15 myrouter alarmd[584]: Alarm cleared: Pwr supply color=RED,
class=CHASSIS, myrouter=Power Supply A fan failed
Apr  8 14:00:18 myrouter scb CM: ALARM CLEAR: Power Supply A fan failed
Apr  8 14:00:21 myrouter alarmd[584]: Alarm set: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply A fan failed
Apr  8 14:00:23 myrouter scb CM: ALARM SET: (Major) Power Supply A fan failed
Apr  8 14:05:16 myrouter alarmd[584]: Alarm set: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply A fan failed
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. Use the show log messages | match "power supply" command to view only power supply error messages. Use this information to diagnose a power supply problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events prior to the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display Power Supply Error Messages in the Chassis Daemon Log File

Action To display power supply error messages in the chassisd log file, use the following CLI command:

user@host> **show log chassisd | match pem**

Sample Output

```
user@host> show log chassisd | match pem
Jul 15 11:18:59 CMB cmd to PEM#0 [0xf8], Amber LED Off [0x18]
Jul 15 11:18:59 PEM#0 - Amber LED Off
Jul 15 11:18:59 CMB cmd to PEM#0 [0xf8], Green LED Off [0x1a]
Jul 15 11:18:59 PEM#0 - Green LED Off
Jul 15 11:18:59 CMB cmd to PEM#0 [0xf8], Blue LED Off [0x16]
Jul 15 11:18:59 PEM#0 - Blue LED Off
Jul 15 11:18:59 CMB cmd to PEM#1 [0xf9], Amber LED Off [0x18]
Jul 15 11:18:59 PEM#1 - Amber LED Off
Jul 15 11:18:59 CMB cmd to PEM#1 [0xf9], Green LED Off [0x1a]
Jul 15 11:18:59 PEM#1 - Green LED Off
Jul 15 11:18:59 CMB cmd to PEM#1 [0xf9], Blue LED Off [0x16]
Jul 15 11:18:59 PEM#1 - Blue LED Off
Jul 15 11:19:02 PEM#0 added
Jul 15 11:19:02 reading PEM 0 initial state
Jul 15 11:19:02 PEM#1 added
Jul 15 11:19:02 reading PEM 1 initial state
Jul 15 11:19:18 CHASSISD_PEM_INPUT_BAD: PEM 1 - INPUT FAIL, status bits: 0xf2,
check breaker
Jul 15 11:19:18 CHASSISD_SNMP_TRAP: SNMP trap: FRU failure: jnxFruContentsIndex
2, jnxFruL1Index 2, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName PEM 1,
jnxFruType 7, jnxFruSlot 2, jnxFruOfflineReason 2, jnxFruLastPowerOff 0,
jnxFruLastPowerOn
26221491, jnxFruPowerUpTime 1484
Jul 15 11:19:23 CHASSISD_PEM_INPUT_BAD: PEM 1 - INPUT FAIL, status bits: 0xf2,
check breaker
```

```
Jul 15 11:19:28 CHASSISD_PEM_INPUT_BAD: PEM 1 - INPUT FAIL, status bits: 0xf2,
check breaker
Jul 15 11:19:33 CHASSISD_PEM_INPUT_BAD: PEM 1 - INPUT FAIL, status bits: 0xf2,
check breaker
Jul 15 11:19:38 CHASSISD_PEM_INPUT_BAD: PEM 1 - INPUT FAIL, status bits: 0xf2,
check breaker
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Verifying Power Supply Failure

Steps To Take To verify a power supply failure, follow these steps:

1. Check the Power Supply Power Switch on page 239
2. Check the Circuit Breaker on page 239
3. Perform a Power Supply Swap Test on page 240
4. Check the Router Cooling System on page 240
5. Test the Power Supply on page 241

Step 1: Check the Power Supply Power Switch

Action If the OK power supply LED is off and no red alarm condition exists, check that the power switch is ON.

Step 2: Check the Circuit Breaker

Action To check the circuit breaker, follow these steps:

1. Verify that the source DC or AC circuit breaker has the proper current rating. Each power supply in the router must be connected to a separate power source.
2. Make sure that the power switch is in the ON (|) position in the circuit breaker box for DC-powered routers. If the circuit breaker box has been tripped, reset it.

Step 3: Perform a Power Supply Swap Test

Action To perform a swap test to determine whether a power supply is defective, follow the procedure in the appropriate router hardware guide to remove the faulty power supply and connect it to a different source with a new power cable. If the power supply does not power on, then the power supply is the source of the problem. Return the faulty power supply for replacement, as described in the appropriate router hardware guide.

CAUTION: When replacing a power supply, do not leave a slot empty for more than two minutes while the router is operational. The power supply must remain in the chassis for proper airflow.

WARNING: Do not touch the power connectors on the back side of the power supply. They can contain dangerous voltages.

Step 4: Check the Router Cooling System

The power supplies require an unobstructed airflow.

If the NO AIRFLOW LED on one of the power supplies lights, check that the airflow around the power supply is sufficient.

Action To check the airflow, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@m40-host> show chassis environment
Class Item                  Status     Measurement
Power Power Supply A        OK
      Power Supply B        Absent

[...Output truncated...]
Fans  Top Impeller          OK         Spinning at normal speed
      Bottom Impeller       OK         Spinning at normal speed
      Rear Fan 1            OK         Spinning at normal speed
      Rear Fan 2            OK         Spinning at normal speed
      Rear Fan 3            OK         Spinning at normal speed

[...Output truncated...]
```

What It Means The command output displays the power supply status and the cooling system status. When monitoring the power supplies, look at both the power supply status and the cooling system status. If the cooling system temperature is above a certain level, the power supplies are automatically cut off.

Alternative Action To check the power supply temperature on M40e and M160 routers, use the following CLI command:

user@host> **show chassis environment pem**

```
user@host> show chassis environment pem
PEM 0 status:
  State                        Online
  Temperature                  OK
  DC input                     OK
  DC output                    OK
  Load                         Less than 20 percent
  Voltage:
    48.0 V input        69028 mV
    48.0 V fan supply   48839 mV
    5.0 V bias           5013 mV
    8.0 V bias           8253 mV
PEM 1 status:
  State                        Online
  Temperature                  OK
  DC input                     OK
  DC output                    OK
  Load                         Less than 20 percent
  Voltage:
    48.0 V input        69307 mV
    48.0 V fan supply   49170 mV
    5.0 V bias           4991 mV
    8.0 V bias           8263 mV
```

The command output displays the temperature of the air flowing past the power supplies (PEMs). The status is either OK or Failed.

To check the status of a specific power supply, indicate the slot number. For example, type show chassis environment pem *slot*, where *slot* can be either 0 or 1.

Step 5: Test the Power Supply

Action On certain power supplies (M5/M10, M40e, and M160 routers), a self-test button is used to test the power supply, It is located beneath the power supply LEDs. The self-test button is for use by qualified service personnel only.

Getting Power Supply Hardware Information

Steps To Take To get the power supply hardware information, follow these steps:

1. Display the Power Supply Hardware Information on page 242
2. Locate the Power Supply Serial Number ID Label on page 242

Step 1: Display the Power Supply Hardware Information

Action To display power supply hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output For M5, M10, M20, M40, and M40e routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                2003              M20
Backplane        REV 07   710-001517   AA7940
Power Supply A   Rev 02   740-001465   000497            AC
Power Supply B   Rev 01   740-001465   000001            AC
[...Output truncated...]
```

For M160 and T320 routers and T640 routing nodes:

```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                47                M160
Midplane         REV 02   710-001245   AB4113
FPM CMB          REV 01   710-001642   AA9721
FPM Display      REV 01   710-001647   AA2995
CIP              REV 02   710-001593   AA9886
PEM 0            Rev 01   740-001243   KJ35782           DC
PEM 1            Rev 01   740-001243   kj35756           DC
[...Output truncated...]
```

What It Means For all routers except the M160 and T320 routers and the T640 routing node, the command output displays the power supply slot number, revision level, part number, serial number, and the power supply type. When facing the back of the router, power supply A is located on the right and power supply B is located on the left.

For the M160 and T320 routers and the T640 routing node, the command output displays the power supply or PEM slot number, revision level, part number, serial number, and power supply type. When facing the back of the router, PEM 0 is located on the right and PEM 1 is located on the left.

Step 2: Locate the Power Supply Serial Number ID Label

Action To locate the power supply serial number ID label, see Table 66 and Figure 95 on page 243 through Figure 101 on page 248.

Table 66: Power Supply Serial Number ID Label Locations on M-series Routers

Router	Power Supply Type	Serial Number ID Label Location
M5 and M10	AC, DC	Power supply faceplate
M7i and M10i	AC, DC	Power supply faceplate
M20	AC, DC	Right side of the power supply back
M40	AC, DC	Top of the power supply

Router	Power Supply Type	Serial Number ID Label Location
M40e	AC	Upper center of the power supply faceplate
	DC	Left center of the power supply faceplate
M160	DC	Left center of the power supply faceplate
M320	AC, DC	On the power supply faceplate under the circuit breaker switch
T320 and T640	DC	Left side of the power supply faceplate

Figure 95 shows the location of the serial number ID label on the power supplies for the M5 and M10 routers. The label is located on the power supply faceplate.

Figure 95: M5 and M10 Router Power Supply Serial Number ID Label

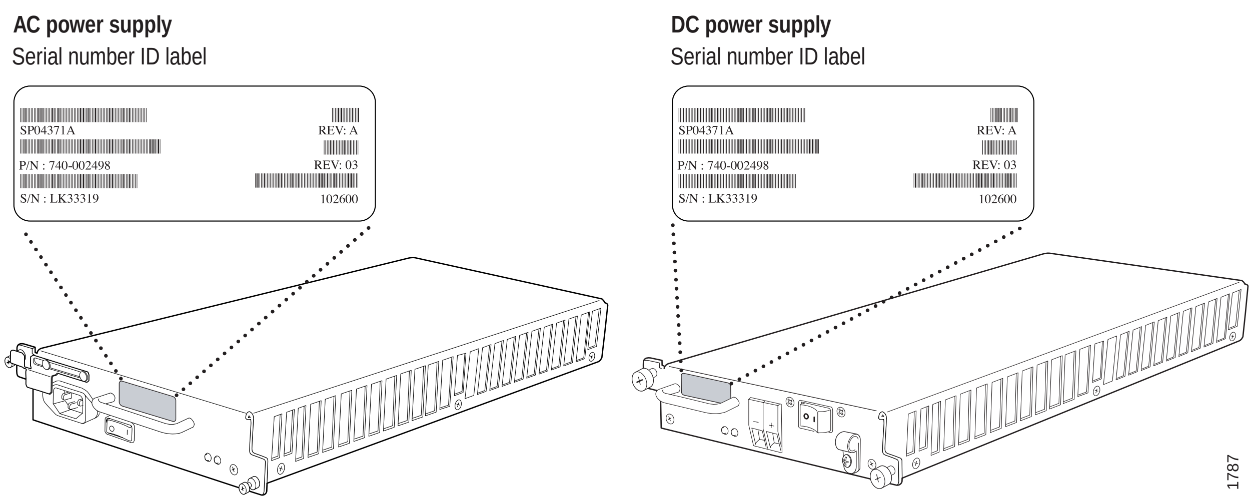


Figure 96 shows the location of the power supply serial number ID label. for the M7i router. The label is located on the power supply faceplate.

Figure 96: M7i Router Power Supply Serial Number ID Label

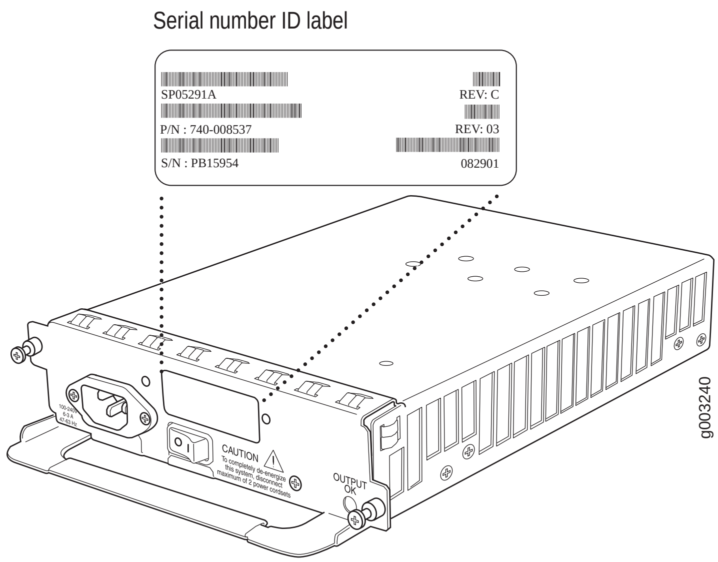


Figure 97 shows the location of the AC and DC power supply serial number ID labels for the M10i router. The labels are located on the power supply faceplate.

Figure 97: M10i Router Power Supply Serial Number ID Labels

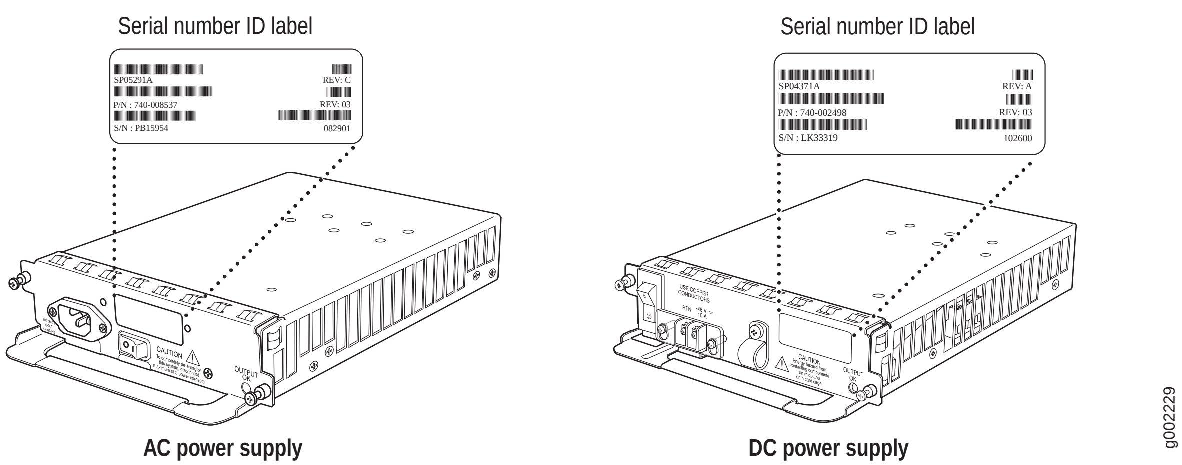


Figure 98 shows the location of the serial number ID label on the power supplies for an M20 router. The label is located on the right side on the back of the power supply.

Figure 98: M20 Router Power Supply Serial Number ID Label

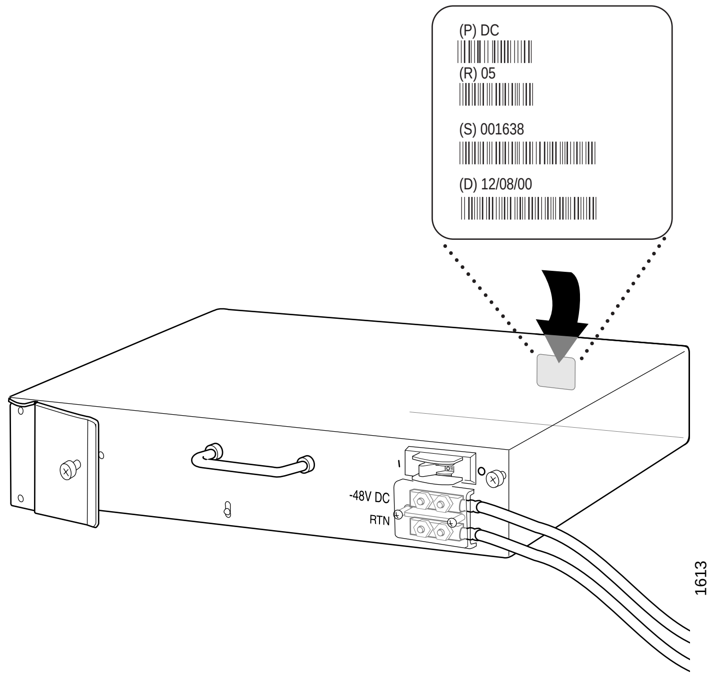


Figure 99 shows the location of the serial number ID label on the power supply for an M40 router. The label is located on the top of the power supply.

Figure 99: M40 Router Power Supply Serial Number ID Label

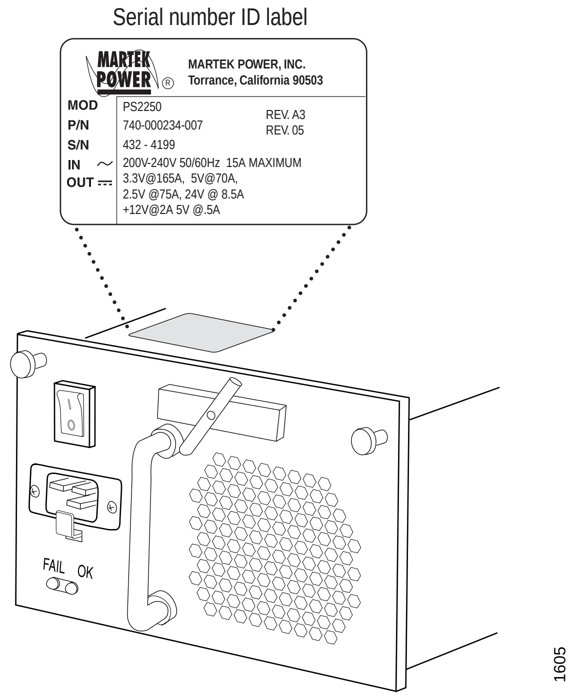


Figure 100 shows the location of the AC power supply serial number ID label for an M40e router. The label is located at the upper center of the faceplate.

Figure 100: M40e Router AC Power Supply Serial Number ID Label

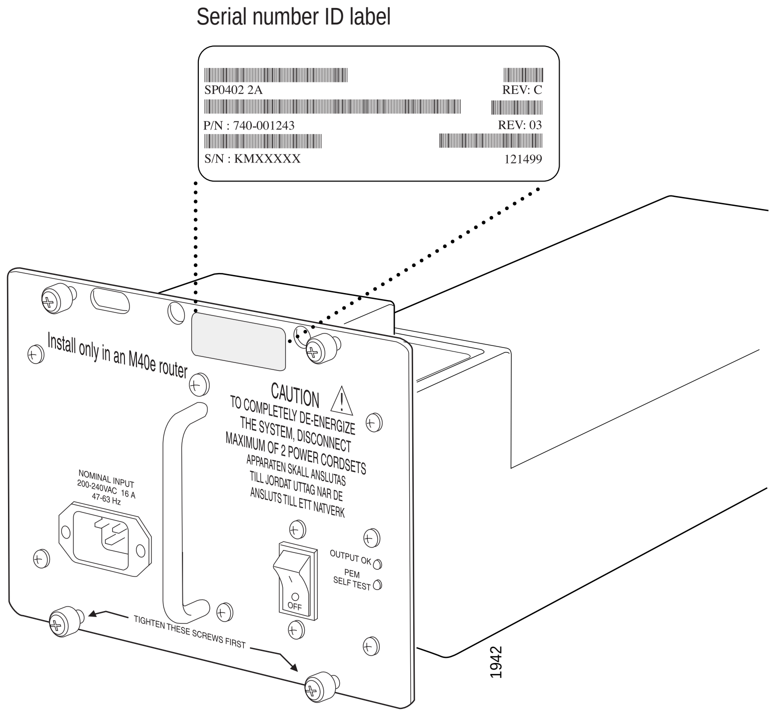


Figure 101 shows the location of the DC power supply serial number ID label for the M40e and M160 routers. The label is located on the faceplate.

Figure 101: M40e and M160 Router DC Power Supply Serial Number ID Label

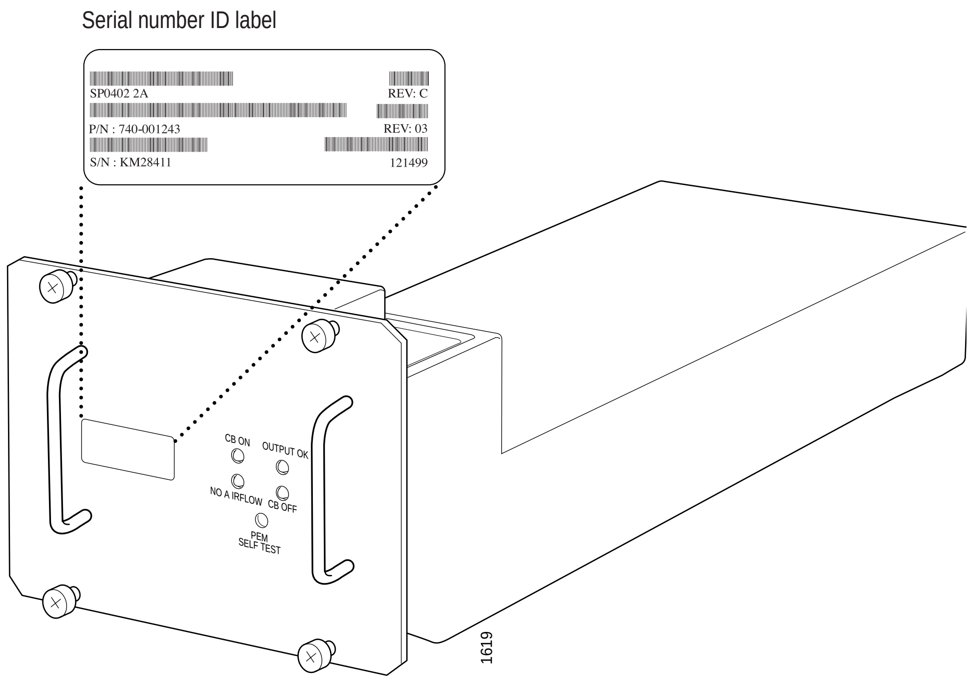


Figure 102 shows the location of the AC and DC power supply serial number ID labels for the M320 router. The serial number ID label is located on the power supply faceplate under the circuit breaker switch.

Figure 102: M320 Router AC and DC Power Supply Serial Number ID Label

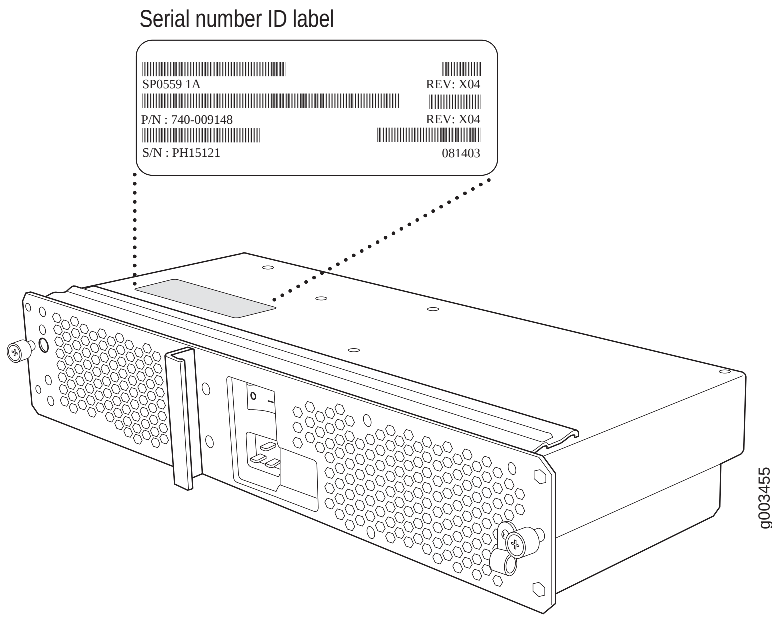


Figure 103 shows the location of the DC power supply serial number ID label for the T320 router. The serial number ID label is located on the left side of the power supply faceplate.

Figure 103: T320 Router DC Power Supply Serial Number ID Label

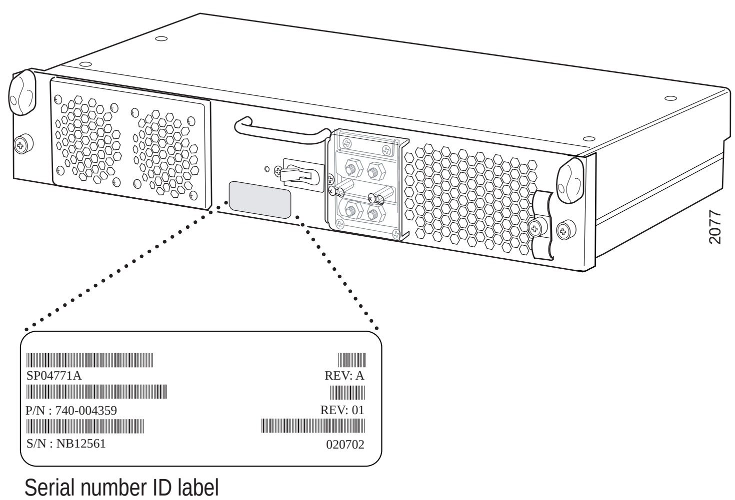
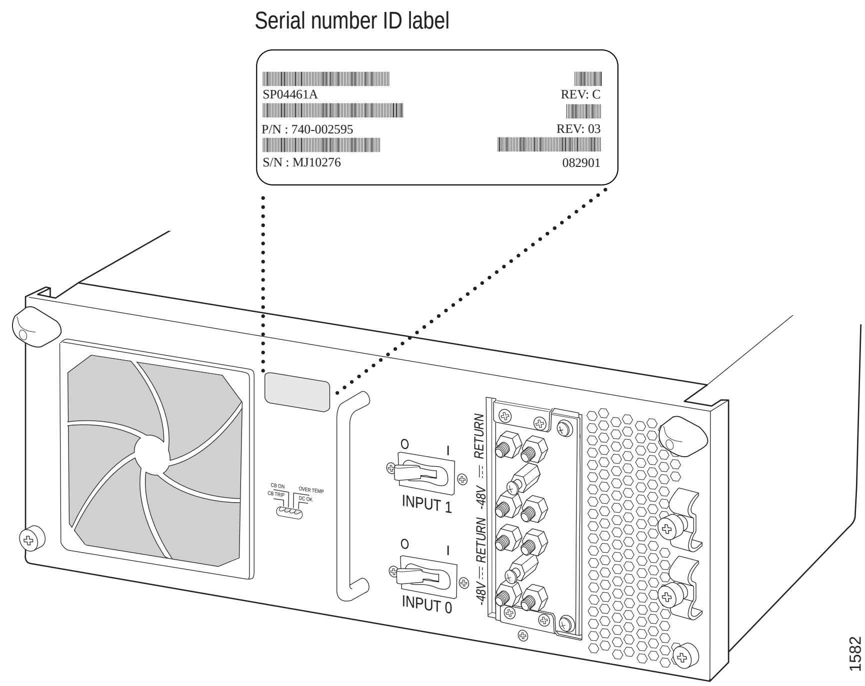


Figure 104 shows the location of the DC power supply serial number ID label for the T640 routing node. The serial number ID label is located on the left side of the power supply faceplate.

Figure 104: T640 Routing Node DC Power Supply Serial Number Label



Replacing the Power Supplies

The power supplies are hot-removable and hot-insertable. You can remove or replace a power supply without powering down the system and disrupting routing functions.

However, you must power down the power supply before removing it from the router. When one power supply is powered down, the other power supply automatically assumes the entire electrical load for the router.

NOTE: The circuit breaker box is not hot-removable or hot-pluggable. You must power down the router to remove the circuit breaker box.

Action To return a failed power supply, see "Return the Failed Component" on page 86. To replace the power supplies, see the appropriate router hardware guide.

Chapter 19

Monitoring the Cooling System

You monitor and maintain the cooling system to keep an acceptable operating temperature for the router chassis and its components. (See Table 67.)

Table 67: Checklist for Monitoring the Cooling System

Monitor Cooling System Tasks	Command or Action
Understanding the Cooling System on page 252	
■ M5 and M10 Router Cooling Systems on page 253 ■ M7i Router Cooling System on page 253 ■ M10i Router Cooling System on page 254 ■ M20 Router Cooling System on page 255 ■ M40 Router Cooling System on page 256 ■ M40e and M160 Router Cooling Systems on page 259 ■ M320 Router Cooling System on page 261 ■ T320 Router and T640 Routing Node Cooling Systems on page 263	
Checking the Cooling System Status on page 267	show chassis environment
Checking the Cooling System Alarms on page 269	
1. Check the Alarm Indicators on the Craft Interface on page 270	show chassis craft-interface Check the router craft interface.
2. Display Current Cooling System Alarms on page 270	show chassis alarms
3. Display Cooling System Error Messages in the System Log File on page 271	show log messages | match fan
Maintaining the Air Filter on page 272	Inspect the air filter. If dirty, clean it; if damaged, replace it.
Verifying a Fan Failure on page 272	Perform a swap test on the fan. If defective, replace it without powering down the router.
Verifying an Impeller Failure on page 273	Feel the impeller air exhaust. If no airflow, replace without powering down the router.
Replacing a Cooling System Component on page 273	Follow the procedure in the appropriate router hardware guide.

Understanding the Cooling System

Purpose Inspect the router cooling system to ensure that air is flowing through the router to cool the components installed in the router chassis. If the router temperature exceeds the critical level, the router automatically shuts down.

What Is the Cooling System The cooling system includes the fans and impellers that provide cooling in the router chassis to keep the components operating at an acceptable temperature.

Table 68 describes the cooling system components for each routing platform.

Table 68: Router Cooling System Components Per Routing Platform

Power Supply Characteristic	M5/ M10	M7i	M10i	M20	M40	M40e	M160	M320	T320	T640
Fan tray	1 with 4 fans	1 with 4 fans	2 with 8 fans each	3 front 1 rear		1	1 lower fan tray	2 front, 1 rear	2 front 1 rear	2 front 1 rear
Power supply integrated fan	_	_	_	2	2	_	Cooled by air flowing through the chassis	_	_	_
Impellers	_	_	_	_	2 pairs	1 central impeller 1 rear upper impeller 1 rear lower impeller	1 upper impeller 2 rear impellers	_	_	_
Fan assemblies	_	_	_	_	3	_	_	_	_	_
Air filter	_	_	_	_	1	1	1	1 front, 1 rear	1 front 1 rear	1 front 1 rear

The following sections describe the various routing platform cooling systems:

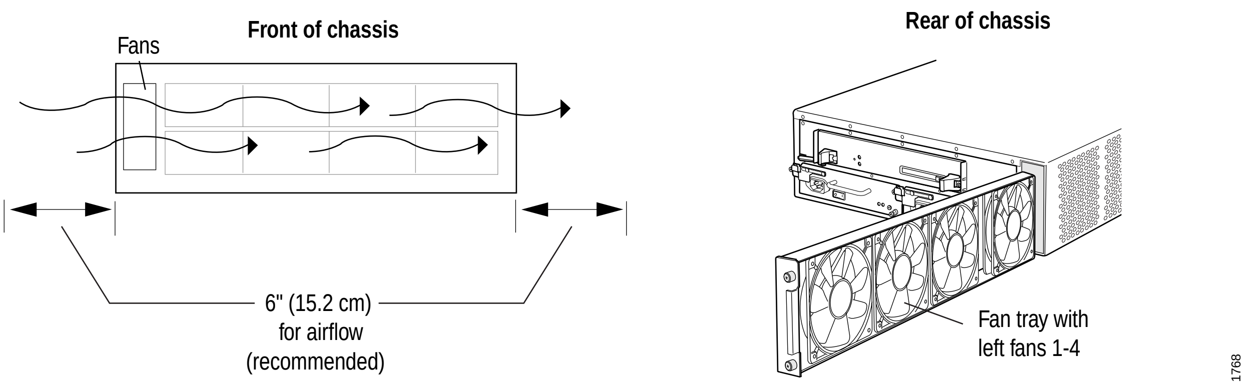
- M5 and M10 Router Cooling Systems on page 253
- M7i Router Cooling System on page 253
- M10i Router Cooling System on page 254
- M20 Router Cooling System on page 255
- M40 Router Cooling System on page 256
- M40e and M160 Router Cooling Systems on page 259
- M320 Router Cooling System on page 261
- T320 Router and T640 Routing Node Cooling Systems on page 263

M5 and M10 Router Cooling Systems

The M5 and M10 router houses four fans, which draw room air into the chassis to keep the internal temperature below a maximum acceptable level. The air flows side-to-side in the chassis (see Figure 105).

CAUTION: Do not remove the fan tray for more than one minute while the router is operating. The fans are the sole source of cooling, and the router can overheat when they are absent.

Figure 105: M5 and M10 Router Cooling System and Airflow

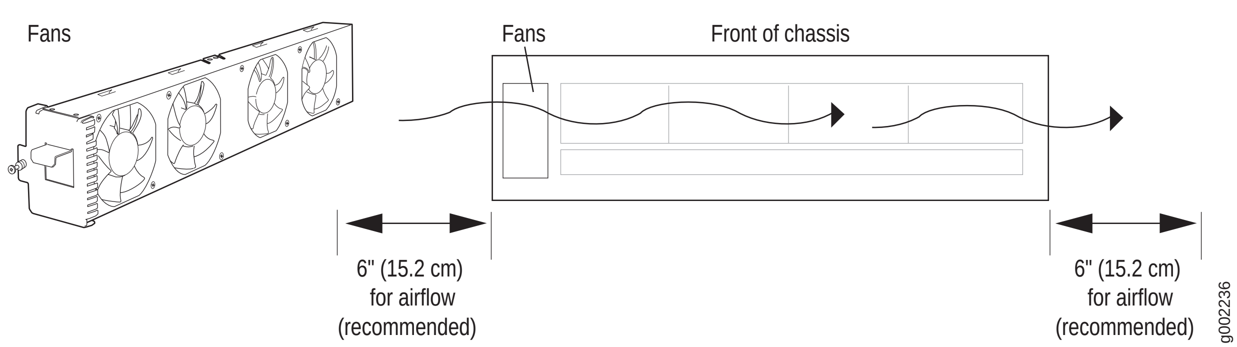


M7i Router Cooling System

The M7i router cooling system consists of a fan tray, located along the left side of the chassis, that provides side-to-side cooling (see Figure 13). It connects directly to the router midplane. The fan tray is a single unit containing four individually fault-tolerant fans. If a single fan fails, the remaining fans continue to function indefinitely.

The cooling system draws in room air through the air intake vent on the left side of the chassis. After entering the chassis, the air stream separates into separate flows for the front and rear components (see Figure 106).

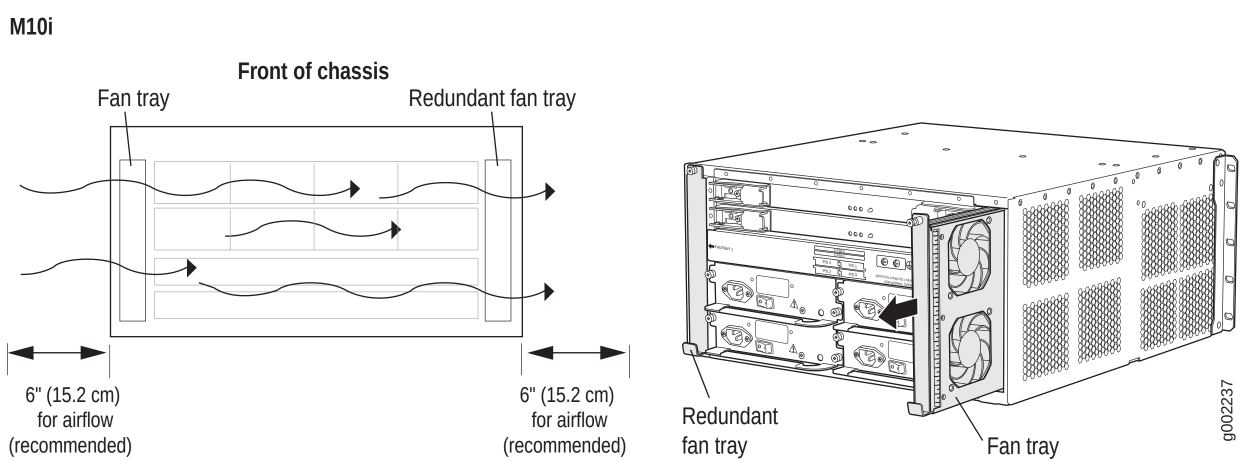
Figure 106: M7i Router Cooling System and Airflow



M10i Router Cooling System

The M10i router cooling system consists of two fan trays, located along the left and right side of the chassis that provide side-to-side cooling. The fan trays house eight fans that draw room air into the chassis to maintain an acceptable operating temperature for the Routing Engine, Physical Interface Cards (PICs), Compact Forwarding Engine Board (CFEB), and other components. The fan trays connect directly to the router midplane. If a single fan fails, the remaining fans continue to function indefinitely (see Figure 107).

Figure 107: M10i Router Cooling System and Airflow



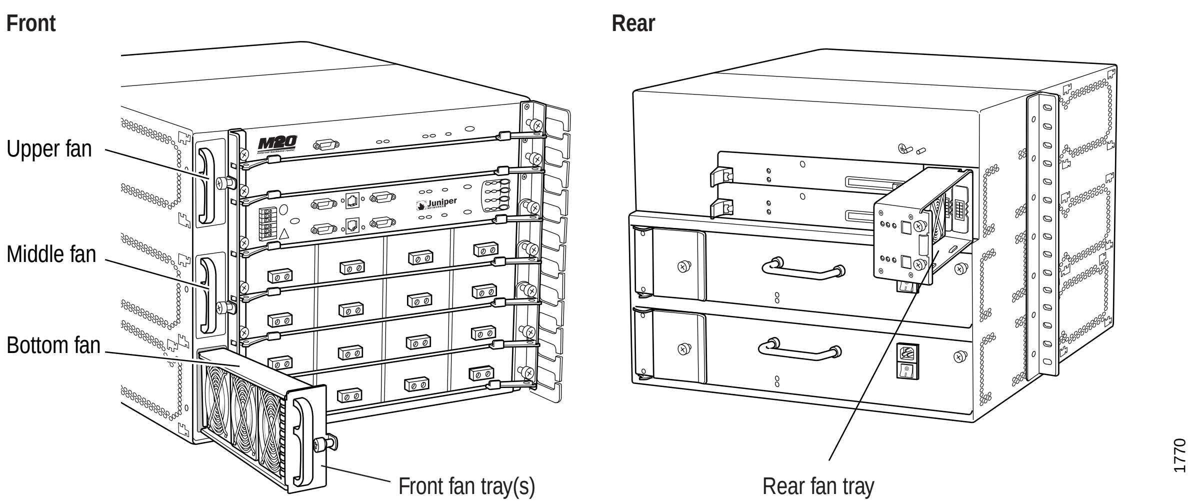
For proper airflow, the primary fan tray should be installed in slot 1 (the left slot looking at the chassis from the rear) and must be installed for proper cooling at all times. The redundant fan tray, if present, should be installed in slot 0 on the right. This fan tray provides additional cooling and redundancy.

M20 Router Cooling System

The M20 router cooling system consists of the following components (see Figure 109):

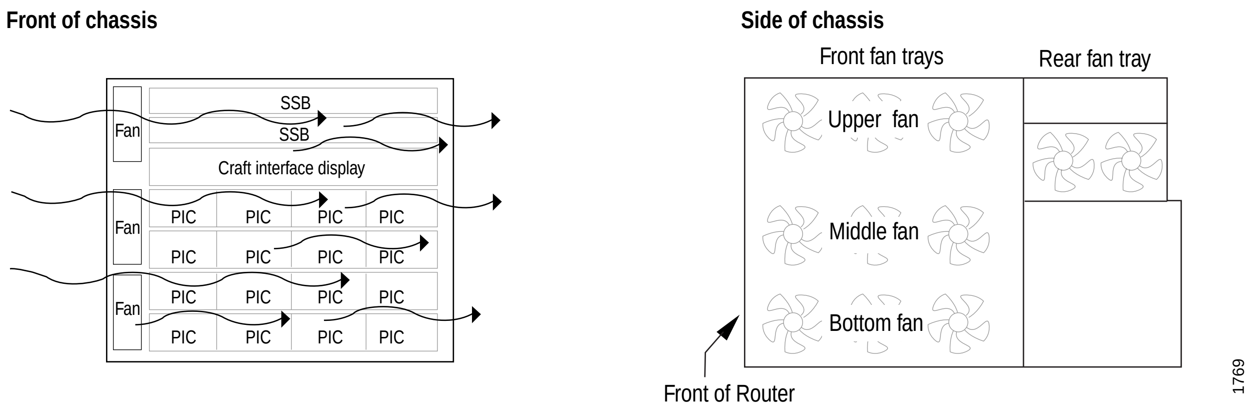
- Three front fan trays—Cool the Flexible PIC Concentrators (FPCs) and the System and Switch Boards (SSBs). The fan trays are located on the left front side of the chassis. Each tray houses three fans.
- Routing Engine fan tray—Cools the Routing Engines. The fan tray is located behind the Routing Engine panel. It houses two fans.
- Power supply integrated fan—Cools each power supply. It is built into the supply.

Figure 108: M20 Router Cooling System Components



The cooling system includes several fan trays that draw room air into the chassis to keep its internal temperature below a maximum acceptable level. The cooling subsystems have redundant components, which are controlled by the SSB. If a fan fails, the remaining fans provide sufficient cooling for the unit indefinitely (see Figure 109.

Figure 109: M20 Router Cooling System and Airflow



M40 Router Cooling System

The M40 router cooling system consists of the following components:

- Air intake vent and air filter (see Figure 111 on page 257)—Provide an opening for room air to enter the router. They are located at the bottom of the chassis front, below the craft interface. The air filter prevents dust and other particles from entering the cooling system. For replacement instructions, see the M40 router hardware guide.

CAUTION: Do not remove the air filter for more than a minute while the router is operating. The fans and impellers are powerful enough to draw in foreign material, such as bits of wire, through the unfiltered air intake, which could damage router components.

- Upper and lower impeller assemblies (see Figure 110 on page 257)—Cool the Packet Forwarding Engine components (backplane, SCB, FPCs, and PICs). The lower impeller assembly is located behind the craft interface at the front the chassis, and the upper assembly is located above the fan tray at the rear of the chassis. Each assembly houses two impellers for redundancy. The assemblies are not interchangeable. For replacement instructions, see the M40 router hardware guide.
- Fan tray (see Figure 111 on page 257)—Cools the Routing Engine and backplane. The tray houses three fans for redundancy and is located above the Routing Engine at the upper rear of the chassis. For replacement instructions, see “Maintain and Replace the Fan Tray” on page 155.
- Power supply integrated fan—Cools the power supply. It is not field-replaceable.

Figure 110 shows the M40 router cooling system impeller trays.

Figure 110: M40 Router Impeller Trays

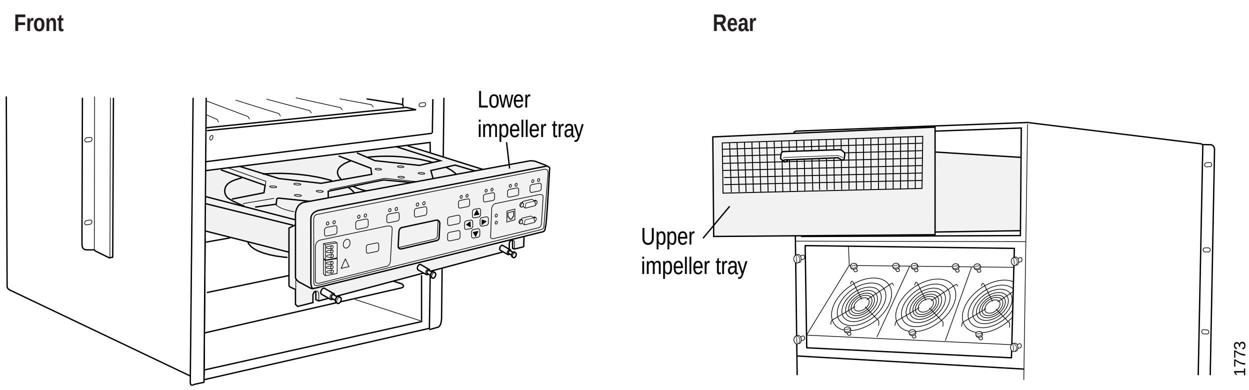
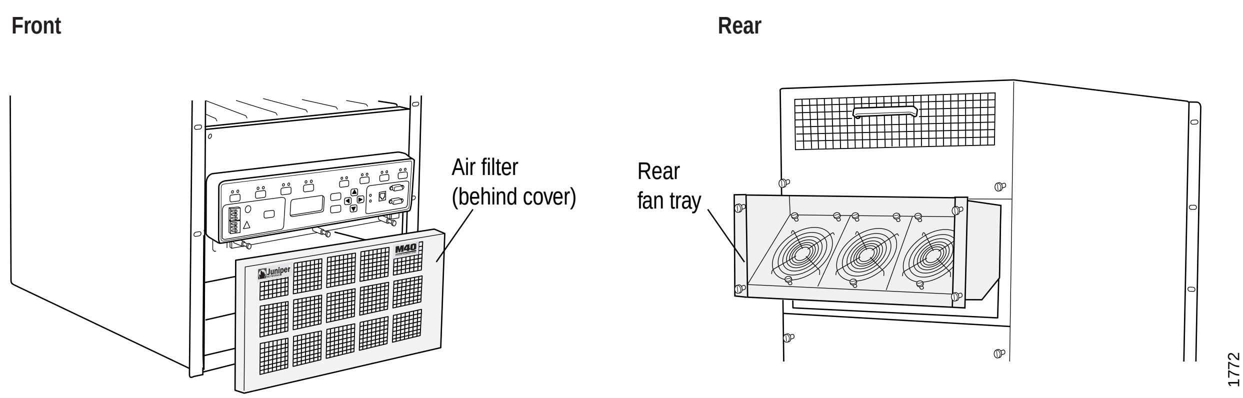


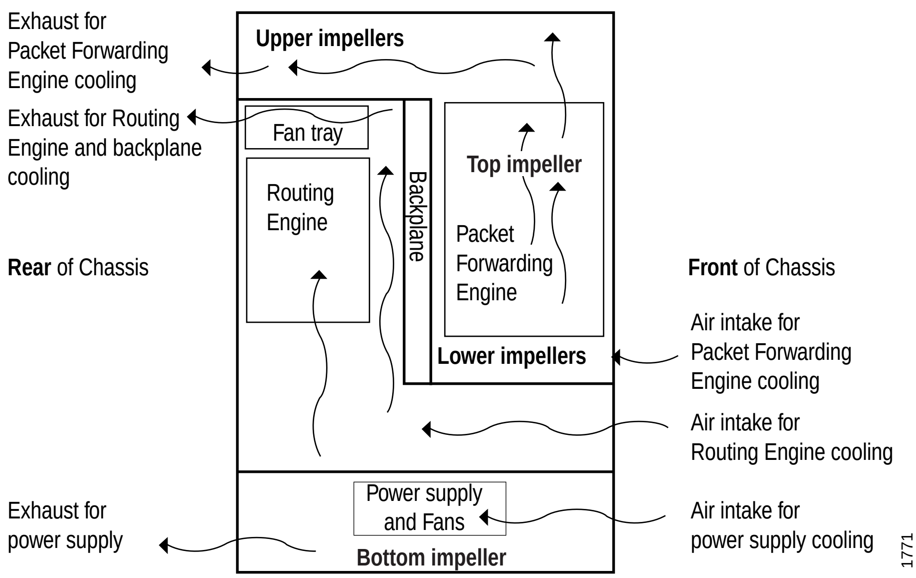
Figure 111 shows the M40 router air filter and fan tray.

Figure 111: M40 Router Air Filter and Fan Tray



The M40 router cooling system consists of separate subsystems (sets of fans and impellers) that draw room air into the chassis to keep its internal temperature below a maximum acceptable level. After entering the chassis, the air stream separates into separate flows for the front and rear subsystems, and the temperature of each flow is monitored independently. Figure 112 shows the M40 router cooling system airflow.

Figure 112: M40 Router Cooling System and Airflow



M40e and M160 Router Cooling Systems

The M40e and M160 router cooling system has the following components:

- Air intake vent, air filter, and intake cover—Provide an opening for room air to enter the router. They are located at the bottom of the chassis front, below the cable management system, as shown in Figure 113 on page 260. The air filter is removable and covers the air intake vent, preventing dust and other particles from entering the cooling system. For maintenance and replacement instructions, see the M40e or M160 router hardware guide. The nonremovable air intake cover is located behind the air filter and provides EMC shielding.

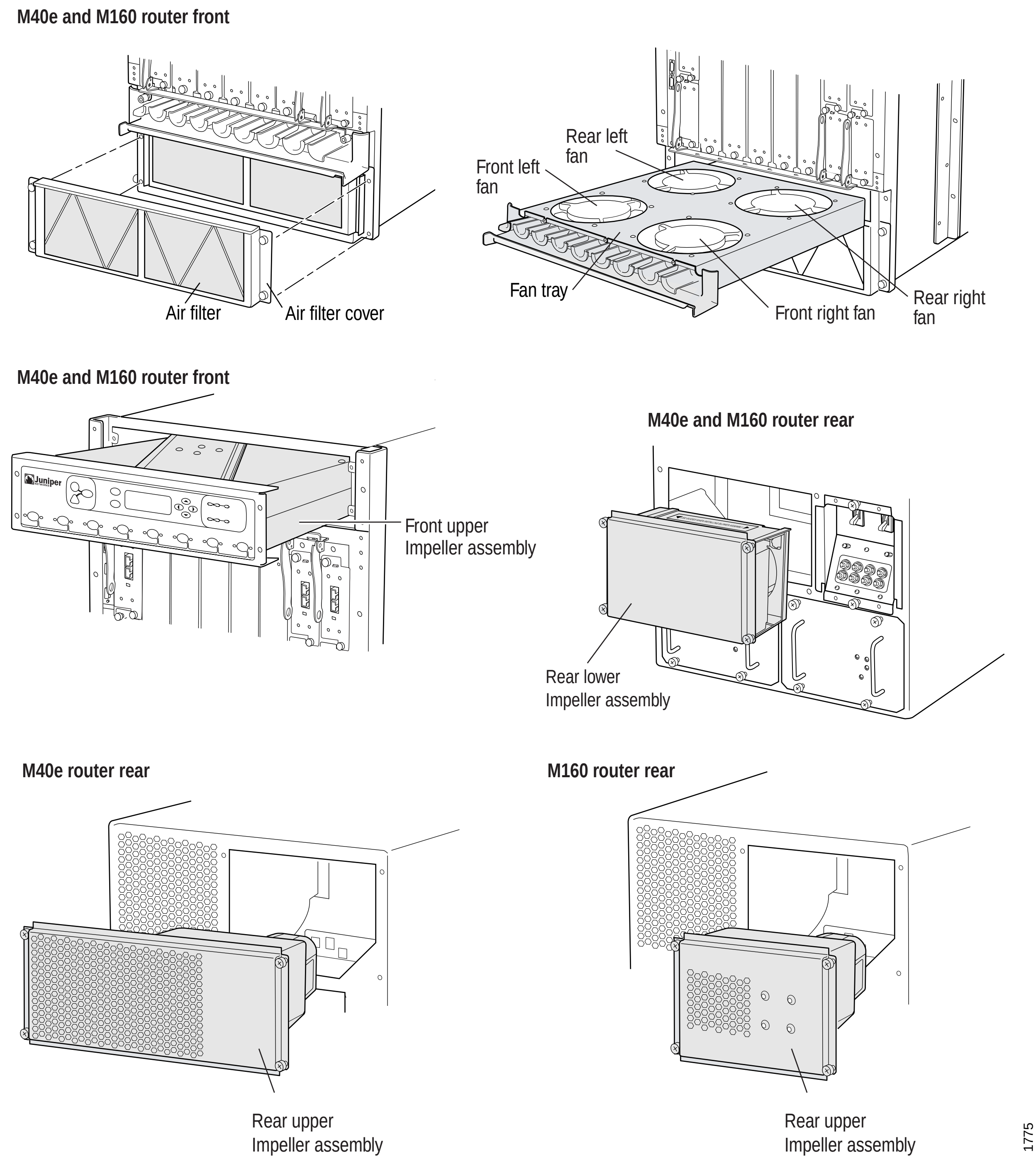
CAUTION: Do not remove the air filter for more than a few minutes while the router is operating. The fans and impellers are powerful enough to draw in foreign material, such as bits of wire, through the unfiltered air intake, which could damage router components.

- Front cooling subsystem—Cools the FPCs, PICs, and midplane. It includes a fan tray located behind the cable management system and a large, central impeller behind the craft interface. For replacement instructions, see the M40e or M160 router hardware guide.

- Rear cooling subsystem—Cools the Switching and Forwarding Modules (SFMs), host module, Packet Forwarding Engine Clock Generator (PCGs), and power supplies. It includes one impeller located at the upper right of the chassis rear and another at the lower left. The upper and lower impellers are not interchangeable. For replacement instructions, see the M40e or M160 router hardware guide.

Figure 113 shows the M40e and M160 router cooling system components.

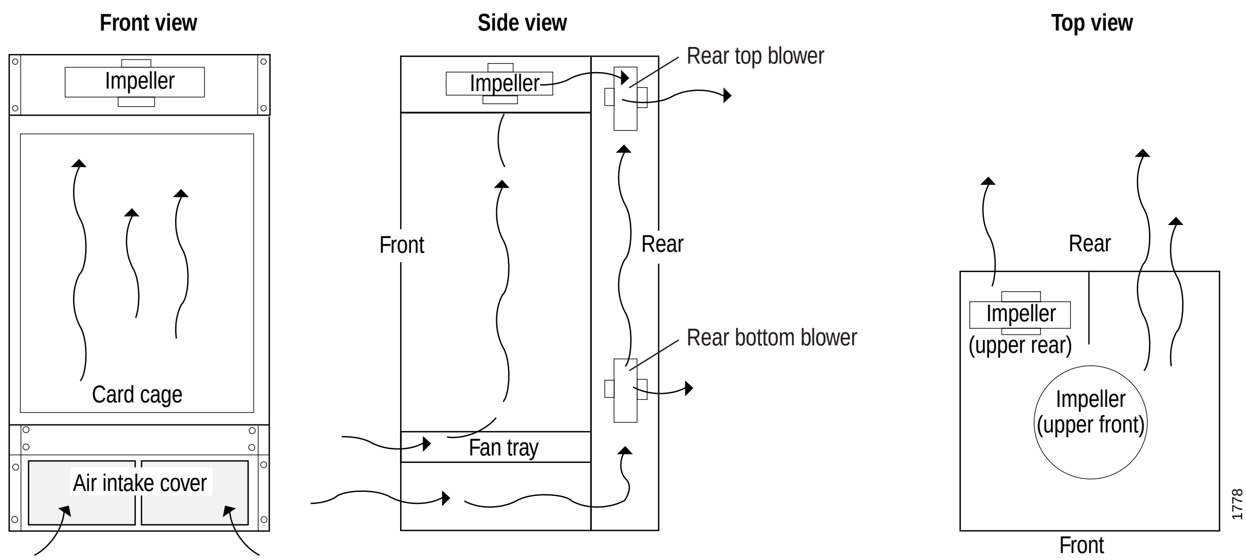
Figure 113: M40e and M160 Router Cooling System Components



The cooling system draws in room air through the air intake vent located at the front of the chassis below the cable management system. After entering the chassis, the air stream separates into separate flows for the front and rear subsystems, and the Miscellaneous Control Subsystem (MCS) monitors the temperature of each flow independently.

Figure 114 shows the M40e and M160 router cooling system components and airflow.

Figure 114: M40e and M160 Router Cooling System and Airflow

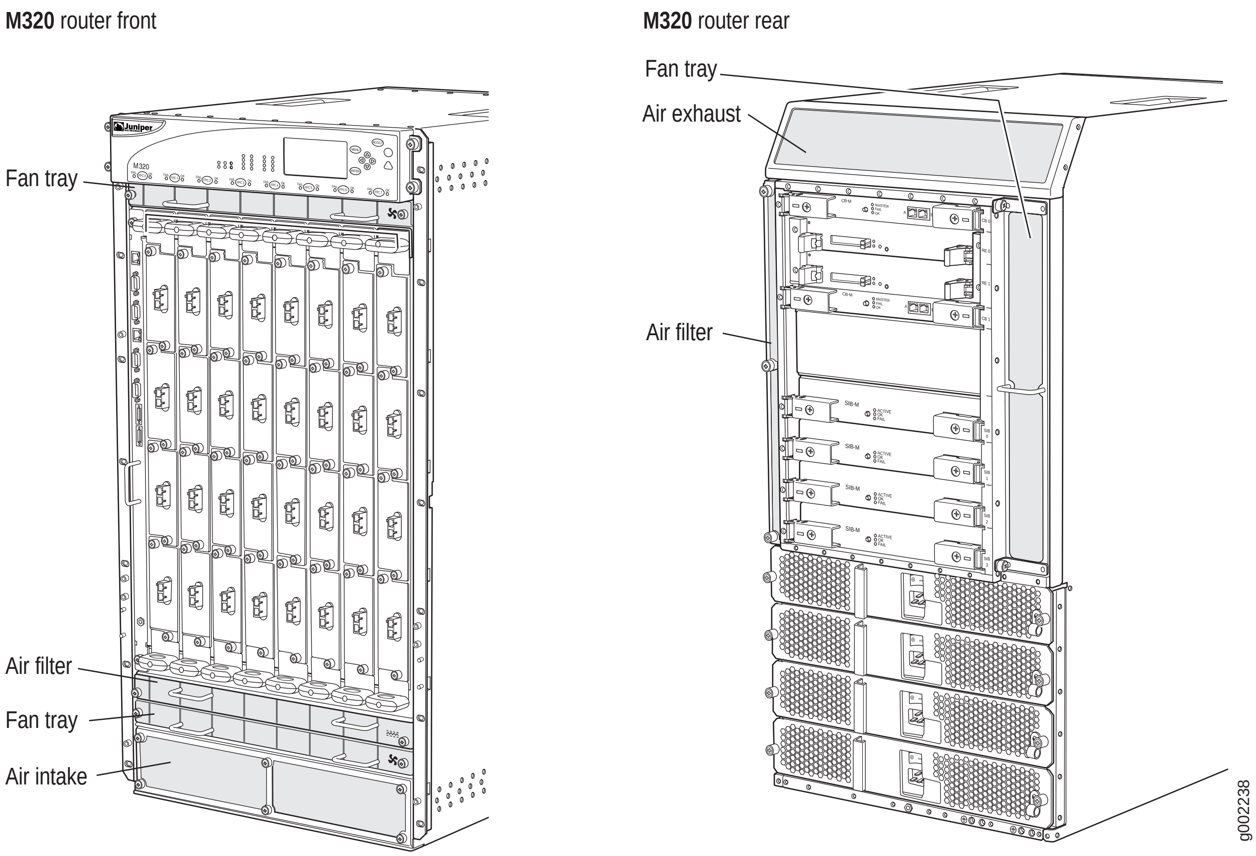


M320 Router Cooling System

The M320 cooling system consists of the following components (see Figure 115 on page 262):

- Two front fan trays—The front fan trays each contain four fans and are interchangeable. The front fan trays cool the components installed in the FPC card cage (the FPCs, PICs, Connector Interface Panel [CIP], and midplane).
- Rear fan tray—The rear fan tray contains seven fans and is not interchangeable with the front trays. The rear fan tray cools the components installed in the rear card cage (the Routing Engines, Control Boards, and the Switch Interface Boards [SIBs]).
- Front and rear air filter—Air filters for both the front and rear fan trays help keep dust and other particles from entering the cooling system.
- Power supply fans—Each power supply has two fans that cool that power supply.

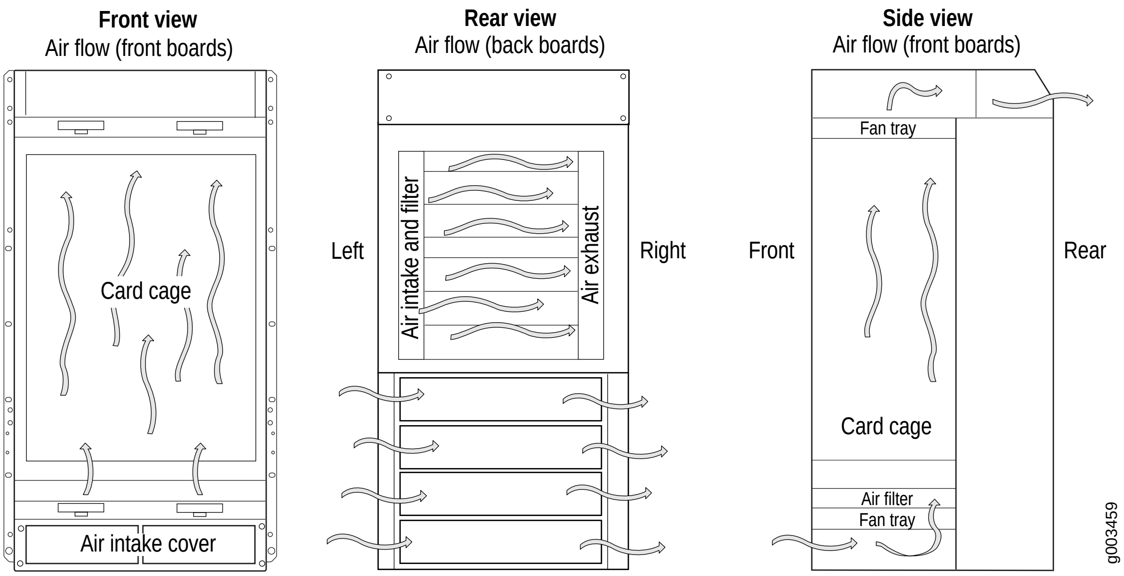
Figure 115: M320 Router Cooling System and Airflow



The host subsystem monitors the temperature of the router components. When the router is operating normally, the fans function at lower than full speed. If a fan fails or the ambient temperature rises above a threshold, the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range. If the ambient maximum temperature specification is exceeded and the system cannot be adequately cooled, the Routing Engine shuts down some or all of the hardware components.

Figure 116 shows the M320 router airflow.

Figure 116: M320 Router Cooling System and Airflow



T320 Router and T640 Routing Node Cooling Systems

The T320 cooling system consists of the following components:

- Two front fan trays—The front fan trays each contain six fans and are interchangeable. The fan trays in the front of the chassis, each with six fans, cool the components installed in the FPC card cage (the FPCs, PICs, CIP, and midplane).
- Rear fan tray—The rear fan tray contains five fans and is not interchangeable with the front trays. It cools the components installed in the rear card cage (the Routing Engines, Control Boards, PCGs, and SIBs).
- Front and rear air filter—Air filters for both the front and rear fan trays help keep dust and other particles from entering the cooling system.
- Power supply fans—The power supplies each have a fan that cools that power supply.

During normal operation, the fans in each fan tray function at less than full capacity. Temperature sensors on the midplane and the host subsystem control the speed of the fans. A fan failure triggers the red alarm LED on the craft interface. If the temperature passes a certain threshold, the JUNOS software turns off the power supplies.

Figure 117 shows the T320 router cooling system components.

Figure 117: T320 Router Cooling System Components

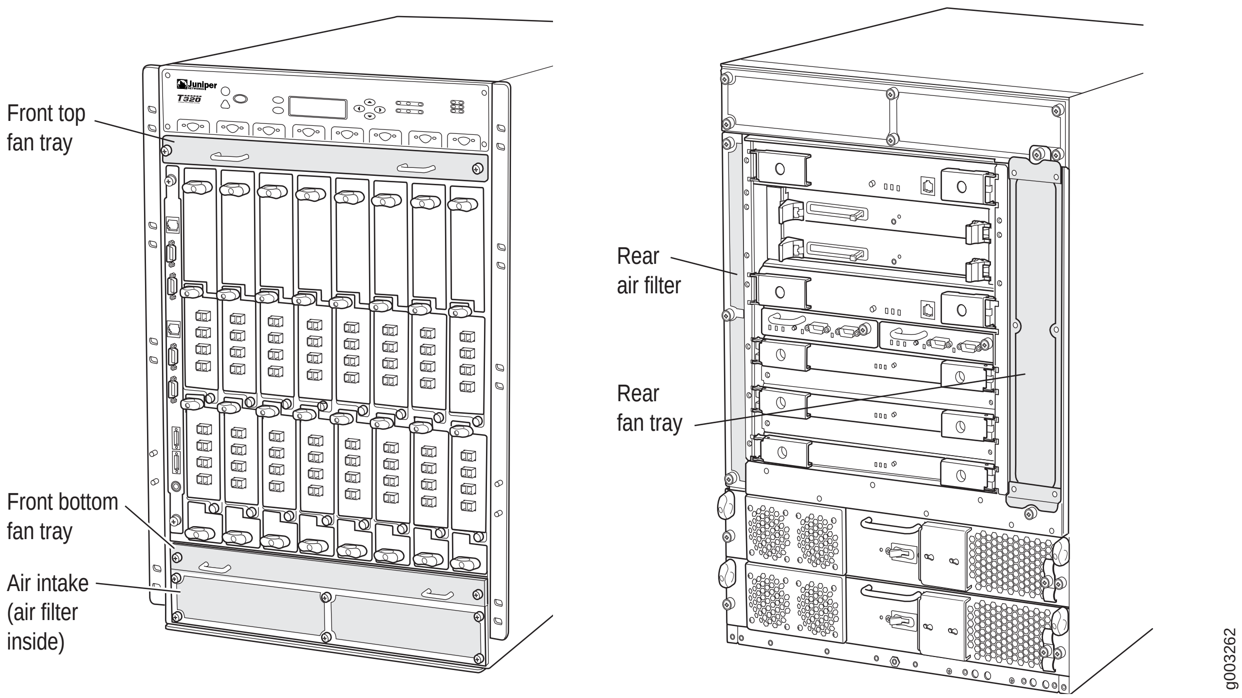


Figure 118 shows the T320 router airflow.

Figure 118: T320 Router Cooling System and Airflow

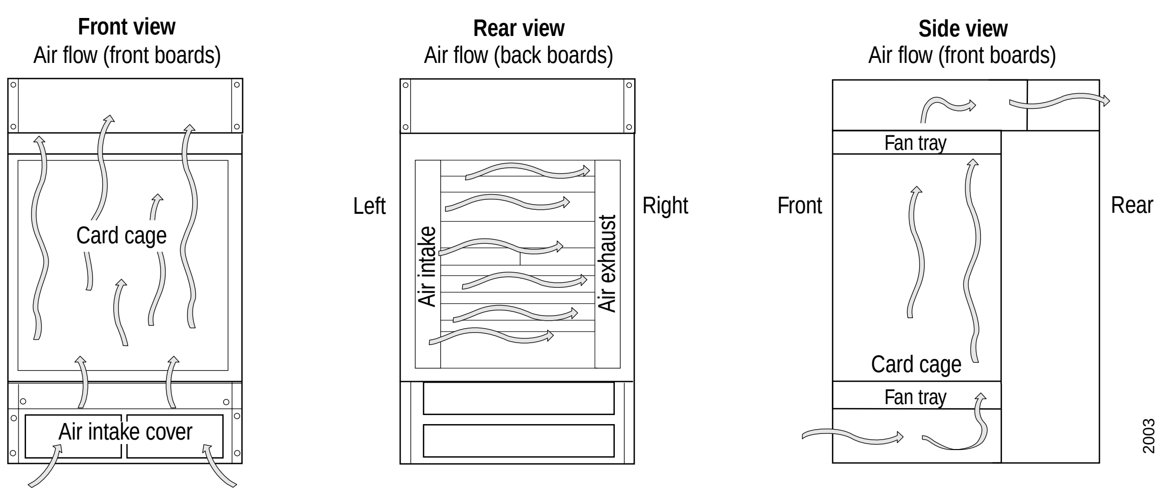


Figure 119 shows the T640 routing node airflow.

Figure 119: T640 Routing Node Cooling System and Airflow

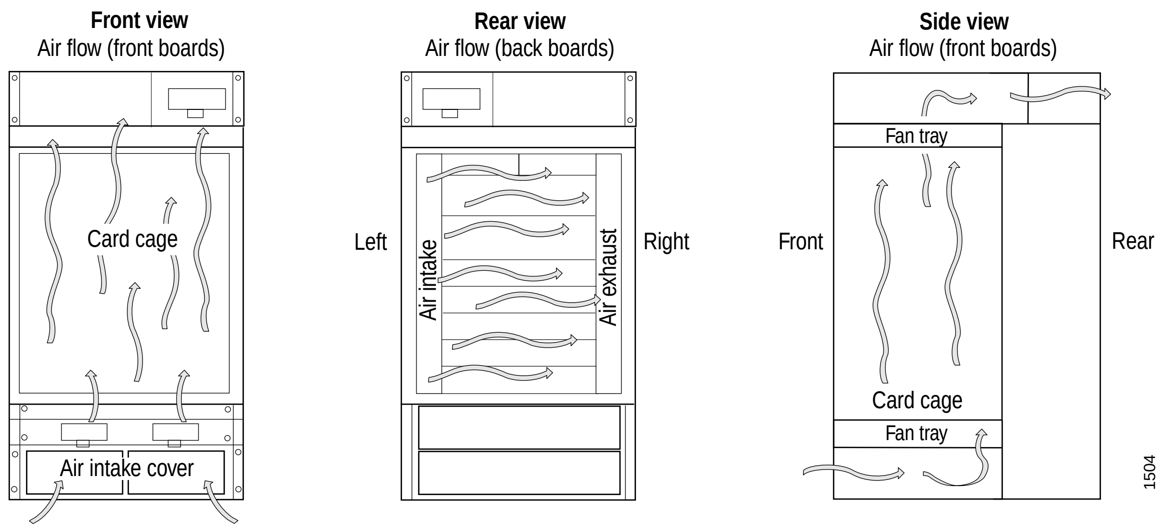
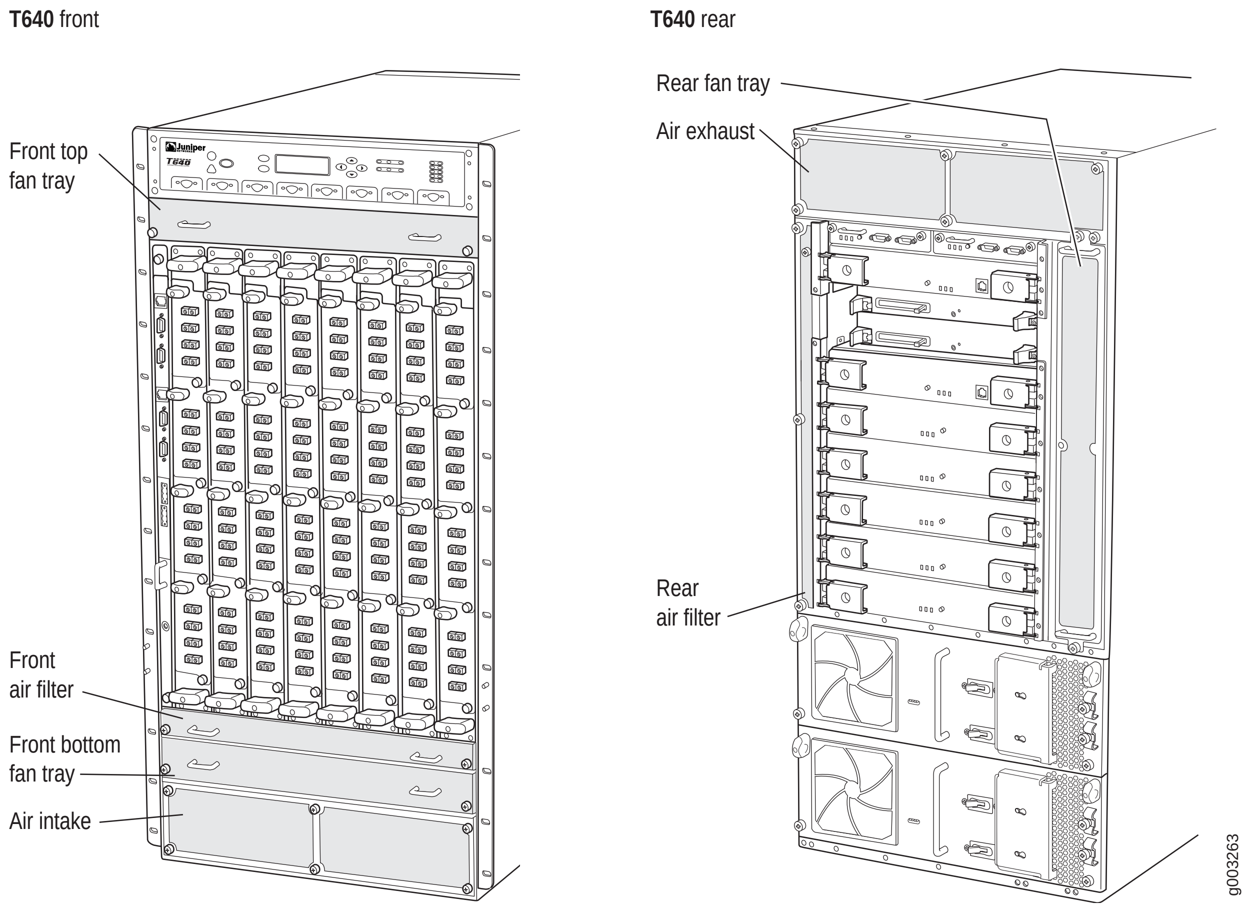


Figure 120 shows the T640 routing node cooling system components.

Figure 120: T640 Routing Node Cooling System Components



See Also "Monitoring Power Supplies" on page 217

Checking the Cooling System Status

For the cooling system to operate properly, the clearance around the chassis must be sufficient for unobstructed airflow. For clearance and maintenance requirements, see the appropriate router hardware guide.

Action To check the cooling system status, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis environment**

Sample Output For M5 and M10 routers (see also Figure 105 on page 253):

```
user@host> show chassis environment
Class Item                    Status     Measurement
[...Output truncated...]
Fans  Left Fan 1              OK         Spinning at normal speed
      Left Fan 2              OK         Spinning at normal speed
      Left Fan 3              OK         Spinning at normal speed
      Left Fan 4              OK         Spinning at normal speed
Misc  Craft Interface         OK
```

For M7i routers (see also Figure 106 on page 253):

```
user@host> show chassis environment
Class Item                    Status     Measurement
[...Output truncated...]
Fans  Fan 1                   OK         Spinning at normal speed
      Fan 2                   OK         Spinning at normal speed
      Fan 3                   OK         Spinning at normal speed
      Fan 4                   OK         Spinning at normal speed
```

For M10i routers (see also Figure 107 on page 254):

```
user@host> show chassis environment
Class Item                    Status     Measurement
[...Output truncated...]
Fans  Fan Tray 0 Fan 1        OK         Spinning at normal speed
      Fan Tray 0 Fan 2        OK         Spinning at normal speed
      Fan Tray 0 Fan 3        OK         Spinning at normal speed
      Fan Tray 0 Fan 4        OK         Spinning at normal speed
      Fan Tray 0 Fan 5        OK         Spinning at normal speed
      Fan Tray 0 Fan 6        OK         Spinning at normal speed
      Fan Tray 0 Fan 7        OK         Spinning at normal speed
      Fan Tray 0 Fan 8        OK         Spinning at normal speed
      Fan Tray 1 Fan 1        OK         Spinning at normal speed
      Fan Tray 1 Fan 2        OK         Spinning at normal speed
      Fan Tray 1 Fan 3        OK         Spinning at normal speed
      Fan Tray 1 Fan 4        OK         Spinning at normal speed
      Fan Tray 1 Fan 5        OK         Spinning at normal speed
      Fan Tray 1 Fan 6        OK         Spinning at normal speed
      Fan Tray 1 Fan 7        OK         Spinning at normal speed
      Fan Tray 1 Fan 8        OK         Spinning at normal speed
```

For an M20 router (see also Figure 109 on page 256):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Rear Fan              OK         Spinning at normal speed
      Front Upper Fan       OK         Spinning at normal speed
      Front Middle Fan      OK         Spinning at normal speed
      Front Bottom Fan      OK         Spinning at normal speed
Misc  Craft Interface       OK
```

For an M40 router (see also Figure 112 on page 258):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Top Impeller          OK         Spinning at normal speed
      Bottom impeller       OK         Spinning at normal speed
      Rear Left Fan         OK         Spinning at normal speed
      Rear Center Fan       OK         Spinning at normal speed
      Rear Right Fan        OK         Spinning at normal speed
Misc  Craft Interface       OK
```

For M40e and M160 routers (see also Figure 114 on page 261):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Rear Bottom Blower    OK         Spinning at normal speed
      Rear Top Blower       OK         Spinning at normal speed
      Front Top Blower      OK         Spinning at normal speed
      Fan Tray Rear Left    OK         Spinning at normal speed
      Fan Tray Rear Right   OK         Spinning at normal speed
      Fan Tray Front Left   OK         Spinning at normal speed
      Fan Tray Front Right  OK         Spinning at normal speed
Misc  CIP                   OK
```

For M320 routers (see also Figure 116 on page 263):

```
user@host> show chassis environment
Class Item                  Status     Measurement
Fan   Top Left Front fan    OK         Spinning at normal speed
      Top Right Rear fan    OK         Spinning at normal speed
      Top Right Front fan   OK         Spinning at normal speed
      Top Left Rear fan     OK         Spinning at normal speed
      Bottom Left Front fan  OK        Spinning at normal speed
      Bottom Right Rear fan  OK        Spinning at normal speed
      Bottom Right Front fan OK        Spinning at normal speed
      Bottom Left Rear fan  OK         Spinning at normal speed
      Rear Fan 1 (TOP)      OK         Spinning at normal speed
      Rear Fan 2            OK         Spinning at normal speed
      Rear Fan 3            OK         Spinning at normal speed
      Rear Fan 4            OK         Spinning at normal speed
      Rear Fan 5            OK         Spinning at normal speed
      Rear Fan 6            OK         Spinning at normal speed
      Rear Fan 7 (Bottom)   OK         Spinning at normal speed
```

For T320 routers and T640 routing nodes (see also Figure 118 on page 264, Figure 117 on page 264, Figure 119 on page 265, and Figure 120 on page 266):

```
user@host> show chassis environment
Class Item                   Status     Measurement
Fans  Top Left Front fan     OK         Spinning at normal speed
      Top Left Middle fan    OK         Spinning at normal speed
      Top Left Rear fan      OK         Spinning at normal speed
      Top Right Front fan    OK         Spinning at normal speed
      Top Right Middle fan   OK         Spinning at normal speed
      Top Right Rear fan     OK         Spinning at normal speed
      Bottom Left Front fan  OK         Spinning at normal speed
      Bottom Left Middle fan OK         Spinning at normal speed
      Bottom Left Rear fan   OK         Spinning at normal speed
      Bottom Right Front fan OK         Spinning at normal speed
      Bottom Right Middle fan OK        Spinning at normal speed
      Bottom Right Rear fan  OK         Spinning at normal speed
      Fourth Blower from top OK         Spinning at normal speed
      Bottom Blower          OK         Spinning at normal speed
      Middle Blower          OK         Spinning at normal speed
      Top Blower             OK         Spinning at normal speed
      Second Blower from top OK         Spinning at normal speed
```

What It Means The command output shows the fans, impellers, or blowers monitored for the router type. The command output displays the fan, impeller, or blower status and the spinning speed. Top Left and Top Right refer to fans in the upper front fan tray; Bottom Left and Bottom Right refer to fans in the lower front fan tray; Blower refers to fans in the rear fan tray. The status can be OK, Testing (during initial power-on), Failed, or Absent. Measurement indicates if the fan or impeller is spinning at normal or high speed.

Checking the Cooling System Alarms

For a listing of cooling system alarm conditions, remedy, and alarm severity by routing platform type, see "Display the Current Router Alarms" on page 61.

Steps To Take To check for cooling system alarms, follow these steps:

1. Check the Alarm Indicators on the Craft Interface on page 270
2. Display Current Cooling System Alarms on page 270
3. Display Cooling System Error Messages in the System Log File on page 271

Step 1: Check the Alarm Indicators on the Craft Interface

Action To check the craft interface alarm indicators, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
Status     Measurement
Red alarm:     LED on, relay on
Yellow alarm:  LED off, relay off
Host OK LED:   On
Host fail LED: Off

[...Output truncated...]
LCD screen:
     +--------------------+
     |myrouter            |
     |2 Alarms active     |
     |R: Fan Failure      |
     |R: Fan Removed      |
     +--------------------+
```

What It Means The command output displays the alarm indicator status. The alarm indicators can be either On or Off. If an indicator is on, an alarm has occurred. The command output also displays the active alarms on the craft interface LCD display. To list the current alarms, use the show chassis alarms command.

Alternative Action You can also physically view the craft interface to see the alarm indicators and alarm descriptions displayed on the LCD display.

Step 2: Display Current Cooling System Alarms

For information that triggers cooling system alarms in each router type, see "Gather Component Alarm Information" on page 60. For fan alarms by router type, see Table 69 on page 271.

Action To display the current cooling system alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
2 alarms currently active
Alarm time               Class  Description
2002-04-08 15:25:12 PDT  Major  Rear left fan stopped spinning
2002-04-08 15:25:12 PDT  Major  Rear left fan Failure
```

What It Means The command output displays the current cooling system alarms, including the time and date stamp, severity level, and description. Table 69 on page 271 shows the possible cooling system alarms for each router type. The alarm LCD short version appears on the craft interface LCD display. The alarm long version appears at the CLI when you use the show chassis alarms command.

Table 69: Cooling System Alarm Messages

Routing Platform	LCD Short Version	CLI Long Version
M5 and M10	N/A	*fan-name* stopped spinning
	N/A	*fan-name* removed
	N/A	Too few fans installed or working
M7i and M10i	N/A	*fan-name* stopped spinning
	N/A	*fan-name* removed
	N/A	Too few fans installed or working
M20	N/A	*fan-name* stopped spinning
	N/A	*fan-name* removed
	N/A	Too few fans installed or working
M40	*fan-name* FAIL	*fan-name* stopped spinning
	fan-name RMVD	*fan-name* removed
	Too few fans	Too few fans installed or working
M40e and M160	Fan Failure	RED ALARM - *fan-name* Failure
	Fan Removed	YELLOW ALARM - *fan-name* Removed
	Fans Missing	RED ALARM - Too many fans missing or failing
T320 and T640	Fan Failure	RED ALARM - *fan-name* Failure
	Fan Removed	YELLOW ALARM - *fan-name* Removed
	Fans Missing	RED ALARM - Too many fans missing or failing

Step 3: Display Cooling System Error Messages in the System Log File

Action To view cooling system error messages in the system log file, use the following CLI command:

user@host> **show log messages | match fan**

Sample Output

```
user@host> show log messages | match fan
Apr  8 14:00:15 myrouter scb CM: ALARM SET: (Major) Power Supply A fan failed
Apr  8 14:00:15 myrouter alarmd[584]: Alarm cleared: Pwr supply color=RED,
class=CHASSIS, myrouter=Power Supply A fan failed
Apr  8 14:00:18 myrouter scb CM: ALARM CLEAR: Power Supply A fan failed
Apr  8 14:00:21 myrouter alarmd[584]: Alarm set: Pwr supply color=RED,
class=CHASSIS, reason=Power Supply A fan failed
Apr  8 14:00:23 myrouter scb CM: ALARM SET: (Major) Rear left fan stopped
spinning
Apr  8 14:05:16 myrouter alarmd[584]: Alarm set: Fan color=RED, class=CHASSIS,
reason=Rear left fan stopped spinning
```

What It Means The messages system log file records the time when the failure or event occurred, the severity level, a code, and a message description. Use the show log messages | match fan command to view only fan error messages. Use this information to diagnose a cooling system problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events prior to the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Maintaining the Air Filter

Action To maintain the air filter on M40, M40e, M160, and T320 routers and T640 routing nodes, follow these steps:

1. Check the air filter for dust, debris, or holes. If the air filter needs cleaning, clean it as described in the appropriate hardware guide.

2. If the air filter needs repair, replace it as described in the appropriate hardware guide.

CAUTION: Because the impellers and fans are quite powerful, it is important to keep the air filter in place while the router is operating. The impellers and fans could pull in foreign material, such as bits of wire, through an unfiltered air intake, resulting in damage to router components.

Verifying a Fan Failure

Action To verify a fan failure, follow these steps:

1. Perform a swap test on the fan. Remove the problem fan tray and put it into another bay. If the fan tray does not work in the other bay, it is probably faulty and must be replaced. If the fan tray works in another bay, there is probably a problem with the power connectivity from the midplane.

2. Check the fan power connector.

3. Check the fan connector on the router midplane.

4. If the fan fails, replace it as described in the appropriate hardware guide. The fans are hot-removable and hot-insertable. You can replace the fans without powering down the router.

NOTE: The cooling system components (fans and impellers) do not have serial numbers. Therefore, you will not see a serial number listed in the hardware inventory or a serial number ID label on the component.

Verifying an Impeller Failure

Action To verify an impeller failure, follow these steps:

1. Place your hand near the exhaust in the router chassis to determine whether the impellers are pushing air out. If you do not feel much air or no air at all, the impeller is not working.

2. If the impeller fails, replace it as described in the appropriate hardware guide. The impellers are hot-removable and hot-insertable. You can replace the fans without powering down the router.

NOTE: The cooling system components (fans and impellers) do not have serial numbers. Therefore, you will not see a serial number listed in the hardware inventory or a serial number ID label on the component.

Replacing a Cooling System Component

The cooling system components are hot-removable and hot-insertable. You can remove or replace a cooling system component without powering down the system and disrupting routing functions. However, you should not operate a router for more than a few minutes without the air filter in place to avoid dust, particles, or other material being sucked into the router chassis.

Action To replace a cooling system component, see the appropriate router hardware guide.

Chapter 20

Maintaining the Cable Management System, Cables, and Connectors

You maintain the router cables in the cable management system to ensure that fiber-optic cables have the proper bend radius and to ensure that all cables are organized and securely in place.

You maintain the Physical Interface Card (PIC) cables and connectors to ensure that they transport incoming packets from the network and transmit outgoing packets to the network.

You maintain the power cables and connectors to ensure that power is supplied to the router.

You maintain the Routing Engine external cables and connectors to ensure that you can connect external devices to the router. (See Table 70.)

Table 70: Checklist for Maintaining Cables and Connectors

Maintain Cable and Connector Tasks	Command or Action
Understanding the Cable Management System, Cables, and Connectors on page 276	
■ M5 and M10 Router Cable Management System on page 277 ■ M10i Router Cable Management System on page 277 ■ M20 Router Cable Management System on page 278 ■ M40 Router Cable Management System on page 279 ■ M40e and M160 Router Cable Management System on page 280 ■ M320 Router Cable Management System on page 280 ■ T320 Router and T640 Routing Node Cable Management System on page 281	
Maintaining the PIC Cables on page 281	Use only specified cables and connectors.
Maintaining the PIC Fiber-Optic Cable on page 282	Follow all guidelines to ensure that fiber-optic cables transmit packets to and from the network.
Cleaning the Transceivers on page 282	Follow all procedures in the cleaning kit you use. See the appropriate router hardware guide and the PIC hardware guide.

Maintain Cable and Connector Tasks	Command or Action
Checking the PIC Port Status on page 283	
1. Check the PIC or FPC LED Status on page 283	Check the PIC LEDs.
2. Display the PIC Media Type on page 284	show chassis fpc pic-status show chassis pic pic-slot *number* fpc-slot *number*
Maintaining the Power Cables on page 285	Use the specified cables and connectors. Turn power off to the router, then reconnect power using the replacement cables.
Maintaining Routing Engine External Cables on page 285	Turn off the power switch, if necessary. Use the specified cable and connector.
Replacing the Cable Management System on page 285	See "Return the Failed Component" on page 86, or follow the procedure in the appropriate router hardware guide.

Understanding the Cable Management System, Cables, and Connectors

Purpose

Inspect the router cables in the cable management system to ensure that fiber-optic cables have the proper bend radius and that all cables are organized and securely in place.

Inspect the PIC cables and connectors to ensure that they transport incoming packets from the network and transmit outgoing packets to the network.

Inspect the power cables and connectors to ensure that power is supplied to the router.

Inspect the Routing Engine external cables and connectors to ensure that you can connect external devices to the router.

What Is the Cable Management System

All Juniper Networks routers have a method of cable management. Although you are not required to use the cable management system, we recommend that you do so. The cable management system maintains the proper bend radius for fiber-optic PIC cables. It keeps installed cables organized, securely in place, and tangle free.

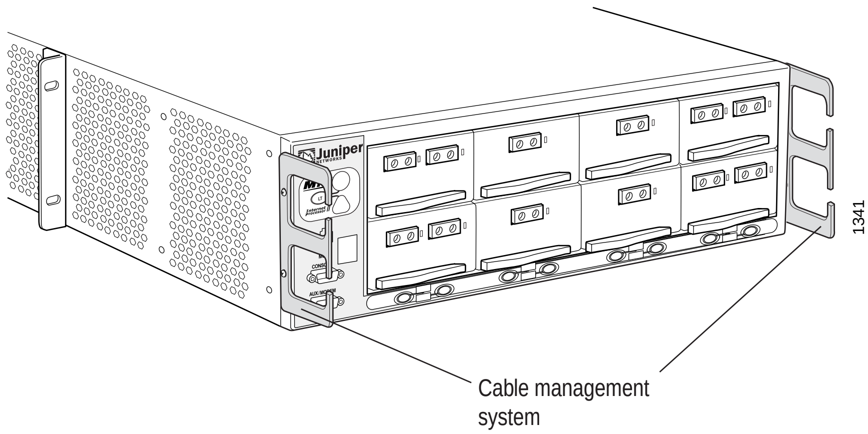
The following sections describe the location of the cable management system on each routing platform.

- M5 and M10 Router Cable Management System on page 277
- M10i Router Cable Management System on page 277
- M20 Router Cable Management System on page 278
- M40 Router Cable Management System on page 279
- M40e and M160 Router Cable Management System on page 280
- M320 Router Cable Management System on page 280
- T320 Router and T640 Routing Node Cable Management System on page 281

M5 and M10 Router Cable Management System

The M5 and M10 router cable management system consists of two vertical pieces, each with a pair of metal hooks draped in a plastic shield, that attach to each side of the front of the chassis. (See Figure 121.)

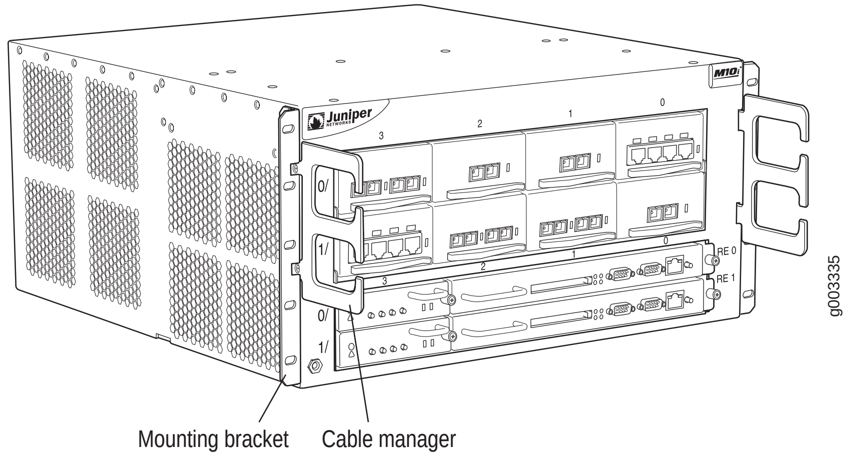
Figure 121: M5 and M10 Router Cable Management System



M10i Router Cable Management System

The M10 router cable management system consists of racks that attach vertically to each side of the chassis at the front, as shown in Figure 122. Pass PIC cables through the slots in the racks to keep the cables organized and securely in place, and to avoid bending optical cables beyond the proper bend radius. The cable management system evenly distributes the weight of a cable, so that it is not subjected to undue stress at the connector.

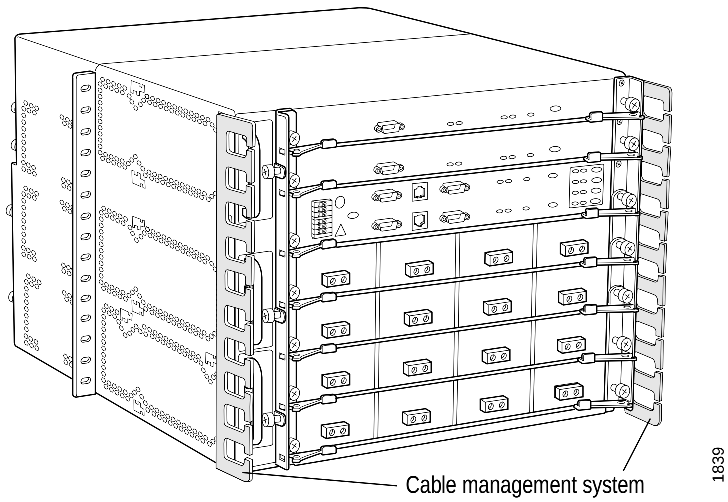
Figure 122: M10i Router Cable Management System



M20 Router Cable Management System

The M20 router cable management system consists of two vertical pieces that attach to each side of the front of the chassis. Each piece consists of a row of staggered metal hooks, each draped with a rounded plastic shield. (See Figure 123.)

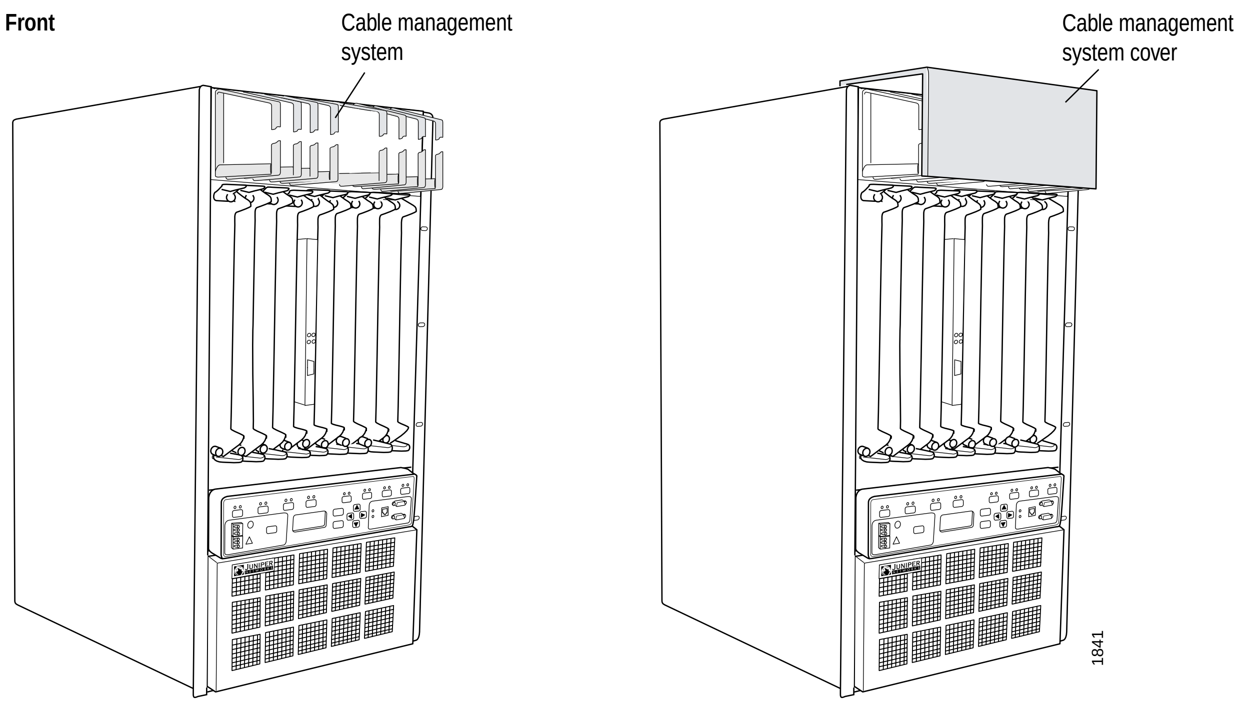
Figure 123: M20 Router Cable Management System



M40 Router Cable Management System

The M40 router cable management system consists of a row of staggered metal hooks, each draped with a rounded plastic shield. The row of hooks is shielded by a removable cable management system cover. (See Figure 124.)

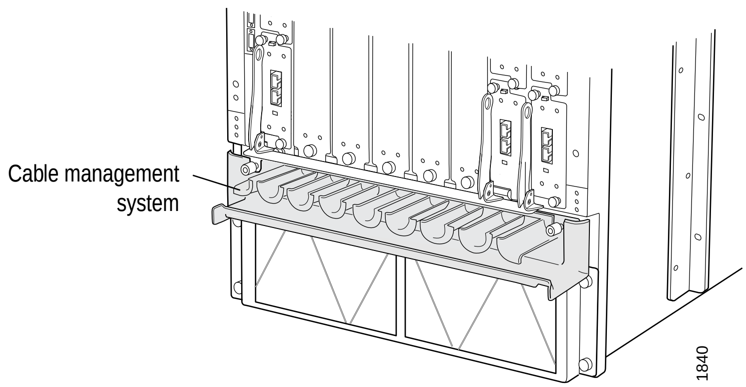
Figure 124: M40 Router Cable Management System and Cover



M40e and M160 Router Cable Management System

The M40e and M160 router cable management system consists of a row of nine semicircular plastic bobbins mounted on the front of the chassis below the Flexible PIC Concentrator (FPC) card cage. PIC cables wrap around the bobbins, keeping the cables organized and securely in place. (See Figure 125.)

Figure 125: M40e and M160 Routers Cable Management System

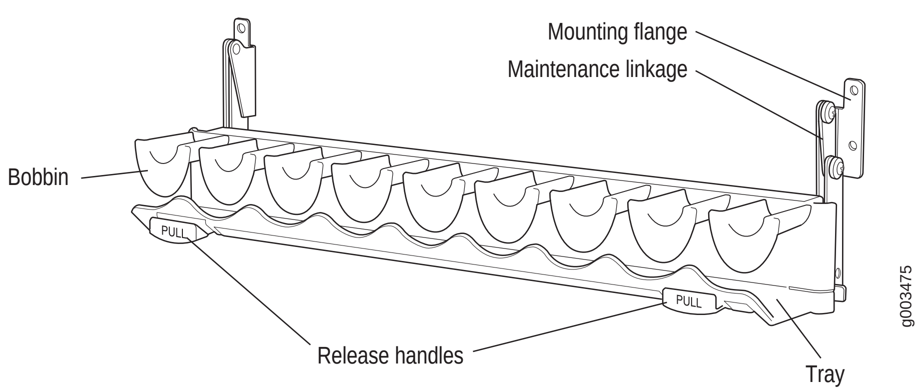


M320 Router Cable Management System

The M320 router cable management system consists of a row of nine semicircular plastic bobbins mounted on the front of the router below the FPC card cage (see Figure 126). The PIC cables pass between the bobbins and into the tray, keeping the cables organized and securely in place. The curvature of the bobbins also helps maintain the proper bend radius for optical PIC cables.

You can pull the cable management system up and outward to lock it into the maintenance position. This allows you to access the lower fan tray and the front air filter.

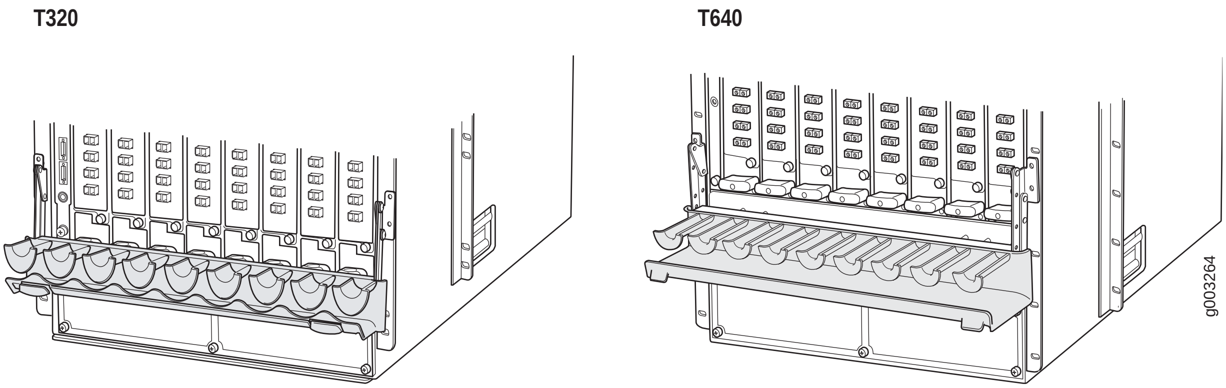
Figure 126: M320 Router Cable Management System



T320 Router and T640 Routing Node Cable Management System

The T320 router and T640 routing node cable management system consists of a row of nine semicircular plastic bobbins mounted on the front of the chassis below the FPC card cage. PIC cables wrap around the bobbins, keeping the cables organized and securely in place. (See Figure 127.)

Figure 127: T320 Router and T640 Routing Node Cable Management System



Maintaining the PIC Cables

Action To maintain the PIC cables, follow these guidelines:

- Make sure that you use the cable and connector type that is specified in the appropriate router hardware guide, especially for the cable and connectors that are not supplied, such as the single-mode interface (fiber) and multimode interface (fiber).
- Make sure that all cable connectors are securely connected. Securely screw in the cable connector screws.
- Use the cable management system to support cables and prevent them from being dislodged or developing stress points.
- Place excess cable out of the way in the cable management system and place fasteners on the loop to help to maintain the shape of the cables. Do not allow fastened loops of cable to dangle from the system, as this stresses the cable at the fastening point.
- Keep the cable connections clean and free of dust and other particles which can cause drops in the received power level. Always inspect cables and clean them if necessary before connecting an interface.
- Label all PIC cables to identify them. Label each end of the cable the same way.

Maintaining the PIC Fiber-Optic Cable

Action To maintain the PIC fiber-optic cable, follow these guidelines:

- Avoid bending fiber-optic cable beyond its bend radius. An arc smaller than a few inches can damage the cable and cause problems that are difficult to diagnose.
- Anchor fiber-optic cable to avoid stress on the connectors. When attaching fiber to a PIC, secure the fiber so it is not supporting its own weight as it dangles to the floor. Never let fiber-optic cable hang free from the connector.
- When you unplug a fiber-optic cable from a PIC, always place a rubber safety plug over the connector.
- Keep fiber-optic cable connections clean using an appropriate fiber-cleaning device, such as the RIFOCS 945/946 Fiber-Optic Connector Cleaning System. Follow the guidelines in the appropriate router hardware guide.
- Frequent plugging and unplugging of fibers into or out of optical instruments, such as SONET or Asynchronous Transfer Mode (ATM) analyzers, can damage the instruments, which are expensive to repair. We recommend attaching a short fiber extension to the optical equipment. Any wear and tear due to frequent plugging and unplugging is then absorbed by the short fiber extension, which is easy and inexpensive to replace.
- If a fiber-optic cable is damaged, replace it as described in the appropriate router hardware guide.

CAUTION: If you do not have a replacement rubber plug in your hand, do not unplug the fiber-optic cable from a PIC. The safety plug keeps the connection clean and prevents accidental exposure to light that might be emitted, which can damage your eyes.

CAUTION: Do not look directly into the PICs installed in the FPC or into the ends of fiber-optic cable. PICs that use SONET/SDH or ATM single-mode fiber-optic cable contain laser light sources that can damage your eyes.

Cleaning the Transceivers

To clean the transceivers, use an appropriate fiber-cleaning device, such as RIFOCS Fiber Optic Adaptor Cleaning Wands (part number 946). Follow the directions for the cleaning kit you use.

After you have cleaned the transceiver on the fiber-optic PIC, make sure that the connector tip of the fiber-optic cable is clean. Use only an approved alcohol-free fiber-optic cable cleaning kit, such as the Opptex Cletop-S® Fiber Cleaner. Follow the directions for the cleaning kit you use.

Checking the PIC Port Status

Steps To Take To check the PIC port status, follow these steps:

1. Check the PIC or FPC LED Status on page 283
2. Display the PIC Media Type on page 284

Step 1: Check the PIC or FPC LED Status

Action To view the PIC port status, look at the PIC or FPC LEDs. You can also use the show chassis fpc pic-status *fpc-slot* or the show chassis pic pic-slot *number* fpc-slot *number* CLI commands.

For M5, M10, and M20 routers, each port on each PIC has one LED, which is located on the PIC faceplate above the optical transceiver. Each LED has four different states, described in Table 71. If the cable is installed properly, the PIC port LED is green.

For M5 and M10 routers, if the Forwarding Engine Board (FEB) detects a PIC failure, it sends an alarm to the Routing Engine.

Table 71: M5, M10, and M20 Router PIC LEDs

Color	State	Description
Red	Fail	PIC is online but the link has failed.
Green	Normal	Port is functioning normally.
Yellow	Problem detected; still functioning	To track the problem, use the command-line interface (CLI).
None	Not enabled	Port is not enabled.

For M7i and M10i routers, check the LEDs on the PIC faceplates. Most PIC faceplates have an LED labeled STATUS. Some PICs have additional LEDs, often one per port. The meaning of the LED states differs for various PICs. Each PIC has an LED on the FIC labeled PICS ON/OFF that shows whether the PIC is online.

For M20 routers, if the FPC that houses the PIC detects a PIC failure, the FPC informs the System and Switch Board (SSB), which in turn sends an alarm to the Routing Engine.

For M40 routers, each FPC has two LEDs that report its status as OK or Fail. The LEDs are located below each FPC, on the craft interface. If there is a PIC failure, the FPC Fail LED lights.

For M40e, M160, and T320 routers and T640 routing nodes, each of the eight FPC slots in the router has two LEDs and an offline button located directly above it on the craft interface. The green LED labeled OK and the red LED labeled FAIL indicate the FPC status, as described in Table 72 on page 284. The offline button, labeled with the FPC slot number (for example, FPC4), prepares the FPC for removal from the router when pressed. Press and hold the button for about 3 seconds until the FAIL LED lights.

Each FPC slot has two LEDs that indicate its status. The FPC LEDs, labeled FPC0 through FPC7, are located along the bottom of the craft interface. Table 72 describes the functions of the FPC LEDs. Each FPC also has a button that you use to take the FPC offline and bring it online. The button is located next to the FPC LEDs on the bottom of the craft interface.

Table 72: M40e, M160, and T320 Routers and T640 Routing Node FPC LEDs

Label	Color	State	Description
OK	Green	On steadily	FPC is functioning normally.
		Blinking	FPC is starting up.
FAIL	Red	On steadily	FPC has failed.

Step 2: Display the PIC Media Type

Action To display the PIC media type, use the following JUNOS operational mode CLI command:

user@host> **show chassis fpc pic-status**

Sample Output

```
user@host> show chassis fpc pic-status
Slot 0 Online
  PIC 0    1x OC-12 SONET, MM
  PIC 1    4x OC-3 SONET, SMIR
  PIC 2    4x E1, BNC
  PIC 3    1x CSTM1, SMIR
Slot 1 Online
  PIC 0    4x CT3
Slot 2 Online
  PIC 0    1x Tunnel
Slot 4 Online
Slot 5 Offline
Slot 6 Online
  PIC 0    1x OC-192 12xMM VSR
```

What It Means The command output displays the status for all FPCs installed in the router and a description of the PICs installed in each FPC, including the number of ports, media type, mode, and reach. The FPCs in slots 0, 1, 2, 4, and 6 are online. The FPC in slot 5 is offline. The PICs installed in the router include SONET, E1, Channelized STM1, CT3, Tunnel, and OC192 media PICs.

PIC 0 is one-port, SONET, OC12, and multimedia.

For more detailed information about PIC types, see the appropriate PIC guide.

Alternative Action To view a particular PIC status, use the show chassis pic pic-slot *number* fpc-slot *number* CLI command:

```
user@host> show chassis pic pic-slot 0 fpc-slot 1
PIC fpc slot 1 pic slot 0 information:
  Type                             1x Tunnel
  ASIC type                        Tunnel FPGA
  State                            Online
  PIC version                  1.2
  Uptime                        4 hours, 40 minutes, 53 seconds
```

Maintaining the Power Cables

Action To maintain the power cables, follow these guidelines:

- Make sure that the power and ground cables on each DC power supply are arranged so that they do not obstruct access to the other power supply or to other router components.
- Periodically inspect the site to ensure that the cables connected to the power supply are securely in place and are properly insulated.
- If power cables are damaged, replace them. To replace power cables, you must disconnect power to the router, then reconnect power using the replacement cables. Follow the guidelines in the appropriate router hardware guide.

Maintaining Routing Engine External Cables

The CIP contains connectors for connecting the Routing Engines to a console, a network, an external management device, or an external alarm device.

Action To maintain the Console or Auxiliary Port cable, the Ethernet Management cable, or the alarm relay cables, see the appropriate router hardware guide.

Replacing the Cable Management System

The cable management system is hot-removable and hot-insertable. You can remove or replace the cable management system without powering down the system and disrupting routing functions.

Action To replace the cable management system, see the appropriate router hardware guide.

Part 4

Monitoring M320 and T320 Router and T640 Routing Node-Specific Components

Chapter 21

Monitoring the Host Subsystem

You monitor and maintain the host subsystem (the Routing Engine and the Control Board) on the routing platform, which provides the routing and system management functions for the router. (See Table 68.)

Table 68: Checklist for Monitoring the Host Subsystem

Monitor Host Subsystem Tasks	Command or Action
Understanding the Host Subsystem on page 290	
■ M320 and T320 Router and T640 Routing Node Routing Engines on page 291	
■ M320 and T320 Router and T640 Routing Node Control Boards on page 292	
■ Host Subsystem Location on page 294	
Checking the Host Subsystem Status on page 295	show chassis craft-interface Look at the LEDs on the craft interface or the component faceplate.
Checking the Routing Engine Status on page 297	show chassis routing-engine show chassis environment routing-engine
Checking the Control Board Status on page 298	show chassis environment cb

This chapter provides basic information about monitoring the host subsystem components: the Routing Engine and the Control Board. For more detailed information about monitoring the Routing Engine, see "Monitoring the Routing Engine" on page 125. For more detailed information about monitoring the Control Board, see "Monitoring the Control Board" on page 301.

Understanding the Host Subsystem

Purpose Inspect the host subsystem to ensure that the Routing Engine and Control Board function properly.

What Is a Host Subsystem The host subsystem provides routing and system management functions on the M320 and T320 routers and the T640 routing node. The host subsystem is comprised of two components: the Routing Engine and the Control Board. For a host subsystem to function, both of these components must be installed and operational.

The Routing Engine maintains the routing tables used by the router and controls the routing protocols that run on the router.

The Control Board provides control and monitoring functions for the router—determining Routing Engine mastership, controlling power, performing reset and SONET clocking for the other router components, monitoring and controlling fan speed, and monitoring system status using I^2C controllers.

You can install one or two host subsystems on the router. You can install one or two Routing Engines. The Routing Engines install into the upper rear of the chassis in the slots labeled RE0 and RE1. If two Routing Engines are installed, one functions as master and the other acts as backup. If the master Routing Engine fails or is removed, and the backup is configured appropriately, the backup restarts and becomes master. The Routing Engines are hot-pluggable. Each Routing Engine requires that a Control Board be installed in the adjacent slot.

The Control Boards install into the upper rear of the chassis in the slots labeled CB0 and CB1. If two Control Boards are installed, one functions as master and the other acts as backup. If the master Control Board fails or is removed, the backup restarts and becomes master. The Control Boards are hot-pluggable. Each Control Board requires a Routing Engine to be installed in the adjacent slot. CB0 installs above RE0, and CB1 installs below RE1. A Control Board does not function if no Routing Engine is present in the adjacent slot.

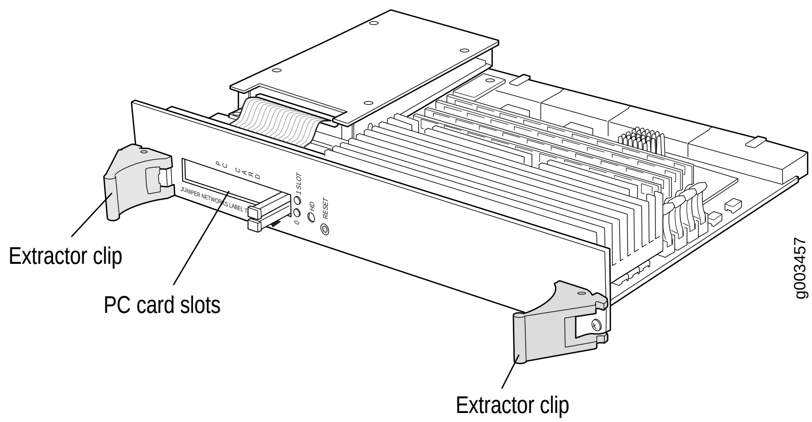
M320 and T320 Router and T640 Routing Node Routing Engines

The following sections describe the Routing Engine component used on each routing platform.

M320 Router Routing Engine

Figure 116 shows the Routing Engine component used on the M320 router.

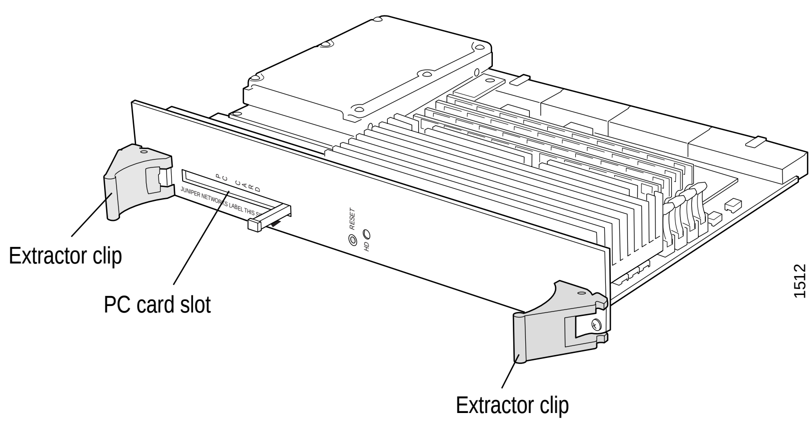
Figure 116: M320 Router Routing Engine Component



T320 Router and T640 Routing Node Routing Engine

Figure 117 shows the Routing Engine component used on the T320 router and T640 routing node.

Figure 117: T320 Router and T640 Routing Node Routing Engine Component



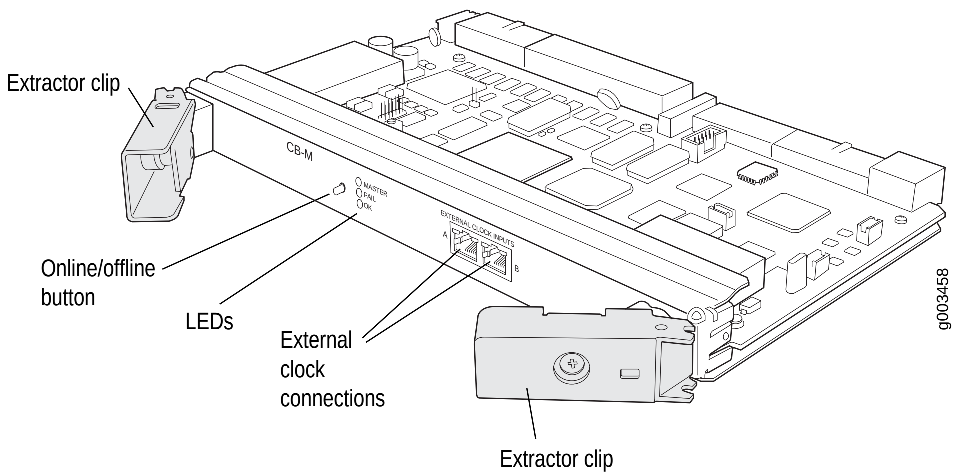
M320 and T320 Router and T640 Routing Node Control Boards

The following sections describe the Control Board used on each routing platform.

M320 Router Control Board

Figure 118 shows the Control Board component used on the M320 router.

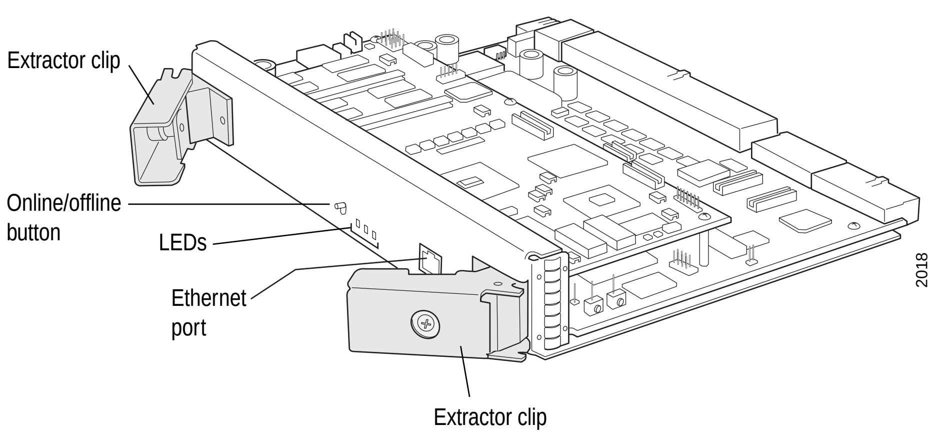
Figure 118: M320 Router Control Board Component



T320 Router Control Board

Figure 119 shows the T320 router Control Board component of the host subsystem.

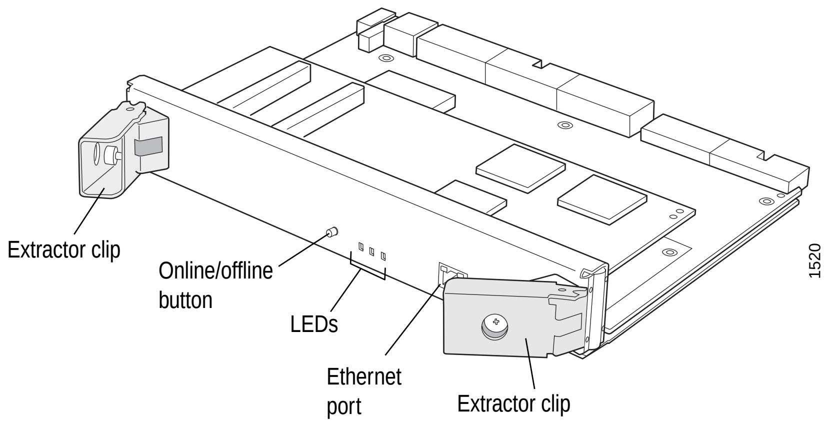
Figure 119: T320 Router Control Board Component



T640 Routing Node Control Board

Figure 120 shows the T640 routing node Control Board component of the host subsystem.

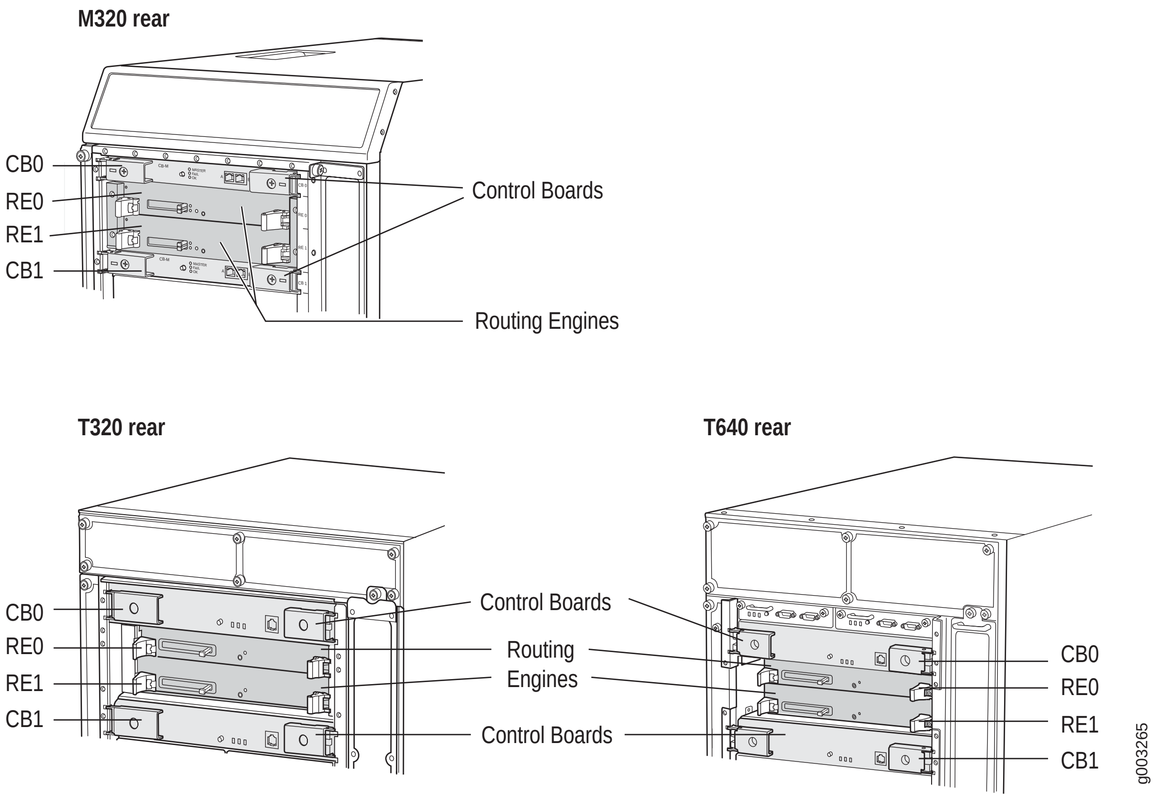
Figure 120: T640 Routing Node Control Board Component



Host Subsystem Location

Figure 121 shows the location of the host subsystem components on the M320 and T320 routers and the T640 routing node.

Figure 121: M320 and T320 Router and T640 Routing Node Host Subsystem Location



You can install one or two host subsystems into the midplane from the rear of the chassis. Each host subsystem functions as a unit: the Routing Engine requires the corresponding Control Board to operate, and vice-versa. If the adjacent component is not present, the Routing Engine or Control Board will not function. RE0 installs below CB0, and RE1 installs above CB1 otherwise the circuit will not be connected.

You take the host subsystem offline and online as a unit. Before you replace a Routing Engine or a Control Board, you must take the host subsystem offline. The host subsystem is hot-pluggable.

See Also

- Monitoring the Routing Engine on page 125
- Monitoring the Control Board on page 301
- Host Redundancy Overview on page 463
- Monitoring Redundant Routing Engines on page 491
- Monitoring Redundant Control Boards on page 559

Checking the Host Subsystem Status

Each host subsystem has three LEDs that display its status. The host subsystem LEDs are located on the right side of the craft interface.

To check the host subsystem status, use the following JUNOS command-line interface (CLI) operational mode command:

user@host> **show chassis craft-interface**

Sample Output

```
m320@host> show chassis craft-interface
FPM Display contents:
    +--------------------+
    |router001|
    |2 Alarms active     |
    |R: PEM 1 Not OK     |
    |R: PEM 0 Not OK     |
    +--------------------|

Front Panel System LEDs:
Routing Engine    0    1
--------------------------
OK                *    *
Fail              .    .
Master            *    .
[...Output truncated...]
```

What It Means On M320 and T320 routers and T640 routing nodes, the Front Panel System LEDs section of the command output shows the Routing Engine status. The state can be OK, Fail, or Master. An asterisk (*) indicates the operating state.

Alternative Actions Check the LEDs on the Routing Engine and the Control Board faceplates at the rear of the router.

Check the Routing Engine or Host Subsystem LEDs on the craft interface. If the red LED is lit, look at the LCD display for more information about the cause of the problem.

Figure 122 shows the location of the Routing Engine LEDs on the M320 router craft interface.

Figure 122: M320 Router Host Subsystem Craft Interface LEDs

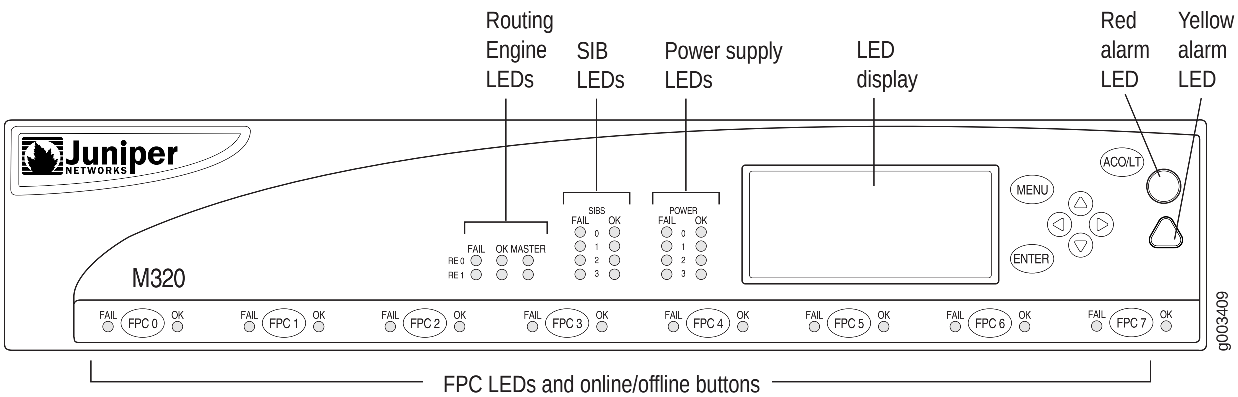


Table 69 describes the M320 router Routing Engine LED states.

Table 69: M320 Router Routing Engine Craft Interface LEDs

Label	Color	State	Description
FAIL	Red	On steadily	Host is offline.
OK	Green	On steadily	Host is online and is functioning normally.
MASTER	Green	On steadily	Host is functioning as master.

Figure 123 shows the location of the Host Subsystem LEDs on the T320 router and T640 routing node craft interface.

Each host subsystem has LEDs, located on the upper right of the craft interface, which indicate its status. The LEDs labeled HOST0 show the status of the Routing Engine in slot RE0 and the Control Board in slot CB0. The LEDs labeled HOST1 show the status of the Routing Engine in slot RE1 and the Control Board in slot CB1.

Figure 123: T320 Router and T640 Routing Node Host Subsystem Craft Interface LEDs

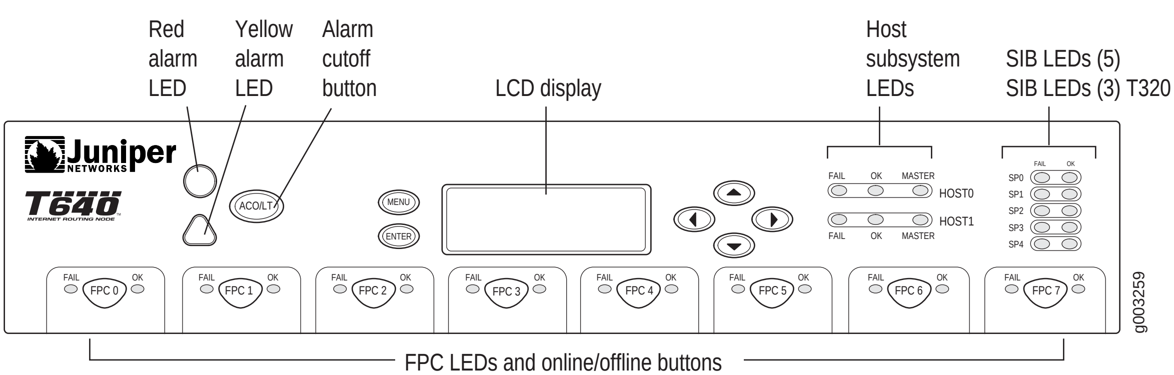


Table 70 describes the T320 router and T640 routing node host subsystem LED states.

Table 70: T320 Router and T640 Routing Node Host Subsystem Craft Interface LEDs

Label	Color	State	Description
OK	Green	On steadily	Host is online and functioning normally.
FAIL	Red	On steadily	Host is offline.
MASTER	Green	On steadily	Host is functioning as master.

Checking the Routing Engine Status

This section provides a brief description of monitoring the Routing Engines as part of the host subsystem on the T320 router and T640 routing node. For more detailed information about monitoring the Routing Engine, see “Monitoring the Routing Engine” on page 125.

Action To check the Routing Engine status, use the following CLI command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 28 degrees C / 82 degrees F
    CPU temperature             27 degrees C / 80 degrees F
    DRAM                      2048 MB
    Memory utilization          11 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     5 percent
      Interrupt                  1 percent
      Idle                      94 percent
    Model                          RE-4.0
    Serial ID                      P11123900322
    Start time                     2004-09-25 19:32:31 PDT
    Uptime                        9 days, 20 hours, 53 minutes, 8 seconds
    Load averages:                 1 minute   5 minute  15 minute
                                       0.00       0.00       0.00
Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 29 degrees C / 84 degrees F
    CPU temperature             30 degrees C / 86 degrees F
    DRAM                      2048 MB
    Memory utilization          10 percent
    CPU utilization:
[...Output truncated...]
```

What It Means The command output displays the Routing Engine slot number, current state (Master, Backup, or Disabled), election priority (Master or Backup), and airflow temperature. The command output also displays the total DRAM available to the Routing Engine processor, the CPU utilization percentage, and the Routing Engine serial number for the slot. Additionally, the command output displays when the Routing Engine started running, how long the Routing Engine has been running, and the time, uptime, and load averages for the last 1, 5, and 15 minutes.

Check the Uptime to ensure that the Routing Engine has not rebooted since it started running.

Alternative Actions To check the Routing Engine environmental status information, such as the operating state, function, and operating temperature, use the following CLI command:

```
user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                          Online Master
  Temperature                 28 degrees C / 82 degrees F
Routing Engine 1 status:
  State                          Online Standby
  Temperature                 29 degrees C / 84 degrees F
```

Check the LCD display on the craft interface to view information about the router temperature and the status of the Routing Engines.

Checking the Control Board Status

This section provides a brief description of monitoring the Control Board as part of the host subsystem on T320 routers and T640 routing nodes. For more information about monitoring the Control Board, see “Monitoring the Control Board” on page 301.

Action To monitor the Control Board environmental status, use the following CLI command:

user@host> **show chassis environment cb**

Sample Output

```
user@host> show chassis environment cb
CB 0 status:
  State                          Online Master
  Temperature                 32 degrees C / 89 degrees F
  Power:
    1.8 V                   1807 mV
    2.5 V                   2473 mV
    3.3 V                   3312 mV
    4.6 V                   4793 mV
    5.0 V                   5008 mV
    12.0 V                 11677 mV
    3.3 V bias              3294 mV
    8.0 V bias              7272 mV
  BUS Revision                16
  FPGA Revision               45
CB 1 status:
  State                          Online Standby
  Temperature                 31 degrees C / 87 degrees F
  Power:
    1.8 V                   1809 mV
```

```
    2.5 V                     2448 mV
    3.3 V                     3305 mV
    4.6 V                     4765 mV
    5.0 V                     4989 mV
    12.0 V                   11633 mV
    3.3 V bias                3284 mV
    8.0 V bias                7301 mV
  BUS Revision                  16
  FPGA Revision                 45
```

What It Means The command output displays environmental information about both Control Boards installed in the router. It displays the Control Board slot, operating status, temperature of air flowing past the Control Board, power supply, and circuitry and field programmable gate array (FPGA) revision information.

The Control Board status can be Present, Online, Offline, or Empty. The command also indicates whether the Control Board is master.

Chapter 22

Monitoring the Control Board

You monitor and maintain the Control Boards that provide control and monitoring functions for the router. These functions include determining Routing Engine mastership, controlling power, performing reset and SONET clocking for the other router components, monitoring and controlling fan speed, and monitoring system status using I^2C controllers. (See Table 71.)

For information on monitoring the Control Boards, see "Monitoring the Host Subsystem" on page 289.

Table 71: Checklist for Monitoring the Control Board

Monitor the Control Board Tasks	Command or Action
Understanding the Control Board on page 303	
■ M320 Router Control Board on page 303 ■ T320 Router Control Board on page 304 ■ T640 Routing Node Control Board on page 304 ■ M320 Router, T320 Router, and T640 Routing Node Control Board Location on page 305	
Monitoring the Control Board Status on page 306	
1. Check the Control Board Environmental Status on page 306	show chassis environment cb
2. Check the Control Board Status from the Craft Interface on page 307	show chassis craft-interface Check the LEDs on the Control Board faceplate. Check the Host Subsystem LEDs on the T320 router and the T640 routing node craft interface.
Checking the Control Board Alarms on page 308	
1. Display Control Board Alarms on page 308	show chassis alarms For conditions that trigger M320 router alarms, see Table 25 on page 74. For conditions that trigger T320 router alarms, see Table 26 on page 77. For conditions that trigger T640 routing node alarms, see Table 27 on page 80.
2. Check the Control Board LEDs on page 309	Look at the LEDs on the Control Board faceplate.
3. Display Control Board Error Messages in the System Log File on page 309	show log messages | match cb
4. Display Control Board Error Messages in the Chassis Daemon Log File on page 309	show log chassisd | match cb

Monitor the Control Board Tasks	Command or Action
Verifying Control Board Failure on page 310	
1. Check the Control Board Connection on page 310	1. Make sure that the Control Board is properly seated in the midplane. 2. Ensure that none of the pins are bent. 3. Check the thumbscrews on the ejector locking tabs.
2. Check the Control Board Fuses on page 311	The fuses for the Control Boards are located in the rear of the midplane behind the power supply in slot PEM0.
3. Perform a Control Board Swap Test on page 312	1. Take the host subsystem offline if the Control Board is master. 2. Replace the Control Board with one that you know works. 3. Bring the Control Board online. 4. Check the Control Board status.
4. Display the Control Board Hardware Information on page 313	show chassis hardware
5. Locate the Control Board Serial Number ID Label on page 314	Look on the bottom of the left side of the Control Board.
Returning the Control Board on page 314	Follow the procedure in the appropriate hardware guide.

Understanding the Control Board

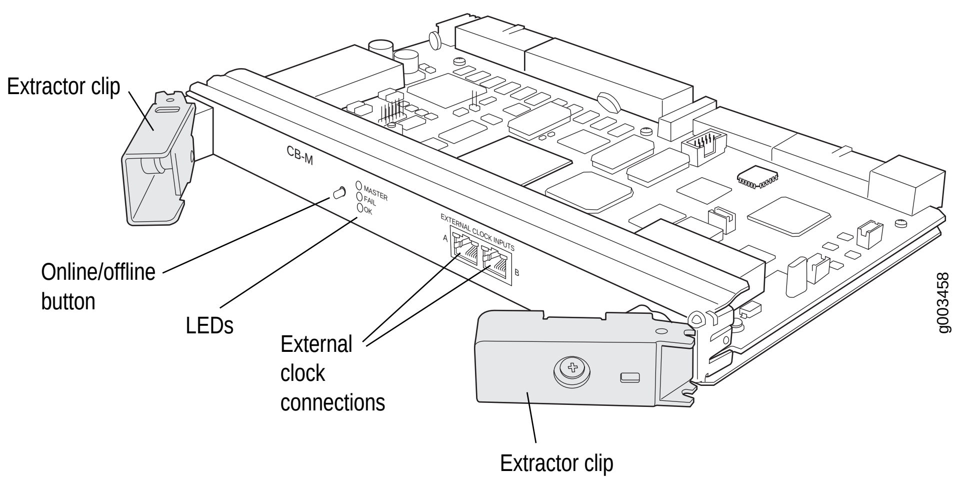
Purpose Inspect the Control Boards to ensure that control and monitoring functions occur for the router.

What Is the Control Board The Control Board works with an adjacent Routing Engine in the host subsystem on M320 and T320 routers and the T640 routing node to provide control and monitoring functions. These functions include determining Routing Engine mastership, controlling power, performing reset and SONET clocking for the other router components, monitoring and controlling fan speed, and monitoring system status using I^2C controllers.

M320 Router Control Board

Figure 124 shows the Control Board component used on the M320 router.

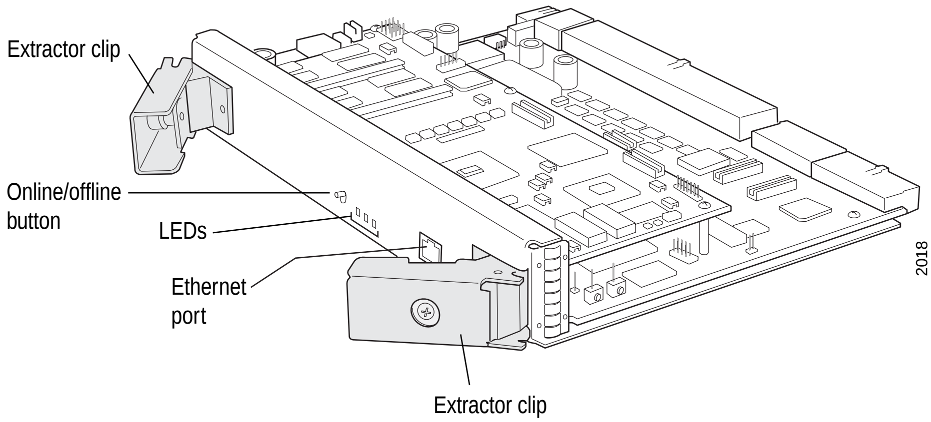
Figure 124: M320 Router Control Board Component



T320 Router Control Board

Figure 125 shows the T320 router Control Board component of the host subsystem.

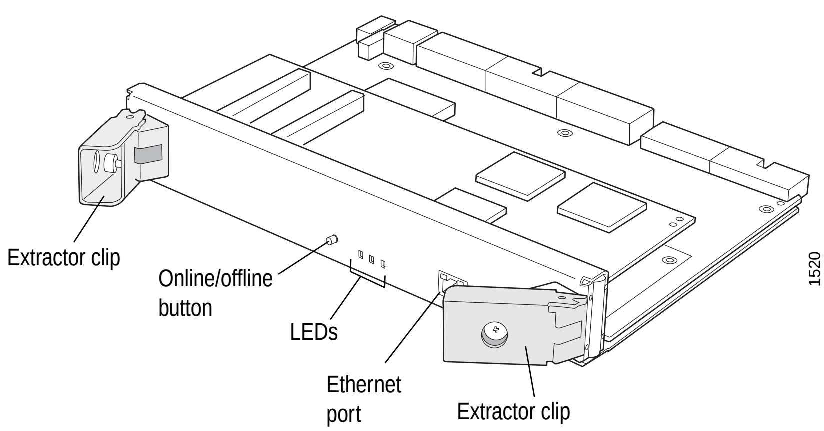
Figure 125: T320 Router Control Board Component



T640 Routing Node Control Board

Figure 124 shows the T320 router Control Board component of the host subsystem.

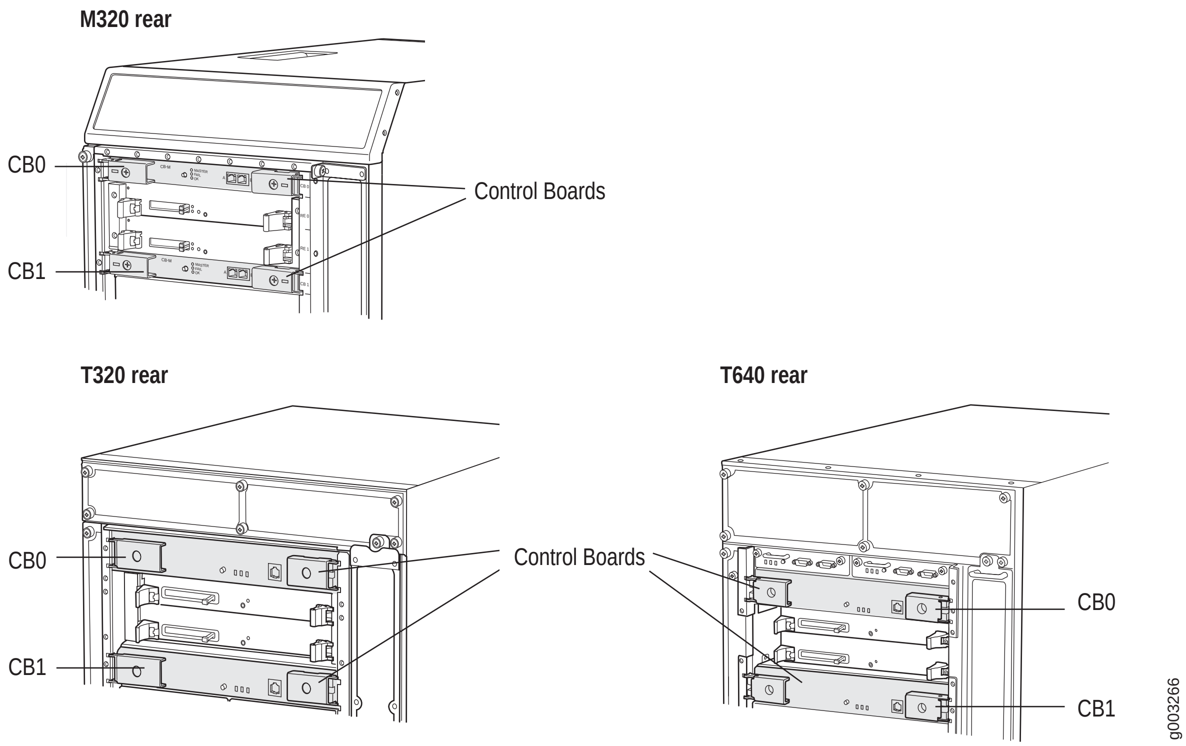
Figure 126: T640 Routing Node Control Board Component



M320, T320 Router, and T640 Routing Node Control Board Location

You can install one or two Control Boards in the router. The Control Boards install into the upper rear of the chassis in the slots labeled CBO and CB1 (see Figure 127).

Figure 127: M320 Router, T320 Router, and T640 Routing Node Control Board Location



Each Control Board requires that a Routing Engine be installed in the adjacent slot. CB0 installs above RE0, and CB1 installs below RE1. A Control Board does not function if no Routing Engine is present in the adjacent slot.

If two Control Boards are installed, one functions as master and the other acts as backup. If the master Control Board fails or is removed, the backup restarts and becomes master.

The Control Boards are hot-pluggable.

See Also

- Monitoring the Control Board on page 301
- Monitoring the Routing Engine on page 125
- Monitoring the Host Subsystem on page 289

Monitoring the Control Board Status

Steps To Take To check the Control Board status, follow these steps:

1. Check the Control Board Environmental Status on page 306
2. Check the Control Board Status from the Craft Interface on page 307

Step 1: Check the Control Board Environmental Status

Action To check the Control Board environmental status, use the following CLI command:

user@host> **show chassis environment cb**

Sample Output

```
t640@host> show chassis environment cb
CB 0 status:
  State                          Online Master
  Temperature                 29 degrees C / 84 degrees F
  Power:
    1.8 V                   1805 mV
    2.5 V                   2501 mV
    3.3 V                   3293 mV
    4.6 V                   4725 mV
    5.0 V                   5032 mV
    12.0 V                 11975 mV
    3.3 V bias              3286 mV
    8.0 V bias              7589 mV
  GBUS Revision               40
  FPGA Revision                7
CB 1 status:
  State                          Online Standby
  Temperature                 32 degrees C / 89 degrees F
  Power:
    1.8 V                   1802 mV
    2.5 V                   2482 mV
    3.3 V                   3289 mV
    4.6 V                   4720 mV
    5.0 V                   5001 mV
    12.0 V                 11946 mV
    3.3 V bias              3274 mV
    8.0 V bias              7562 mV
  GBUS Revision               40
  FPGA Revision                7
```

What It Means The command output lists the Control Board state, redundancy status, temperature, power supply voltages, and circuitry revision level. If you do not specify a Control Board slot number, the command displays the environmental status for each Control Board installed in the router chassis. If you specify a Control Board slot number, the command displays the status for that slot only.

Step 2: Check the Control Board Status from the Craft Interface

Action To check the Control Board operation status from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
t640@host> show chassis craft-interface
FPM Display contents:
[...Output truncated...}
CB LEDs:
  CB   0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .
[...Output truncated...]
```

What It Means The sample output shows that the routing platform has two Control Boards online and functioning normally. The Control Board installed in slot 0 is functioning as master. If an amber asterisk displays, the Control Board has failed.

Alternative Action To view the Control Board status, you can do one of the following:

- (T320 router and T640 routing node) Look at the router craft interface host module status or look at the LCD display for any Control Board alarms.

  Table 72 describes the T320 router and T640 routing node host subsystem LED states.

Table 72: T320 Router and T640 Routing Node Host Subsystem Craft Interface LEDs

Label	Color	State	Description
OK	Green	On steadily	Host is online and functioning normally.
FAIL	Red	On steadily	Host is offline.
MASTER	Green	On steadily	Host is functioning as master.

- Look at the Control Board LEDs on the faceplate. See Figure 127 on page 305 for the Control Board location. For more information, see "Check the Control Board LEDs" on page 309.

Checking the Control Board Alarms

Steps To Take To check for Control Board alarms, follow these steps:

1. Display Control Board Alarms on page 308
2. Display Control Board Error Messages in the System Log File on page 309
3. Display Control Board Error Messages in the Chassis Daemon Log File on page 309

Step 1: Display Control Board Alarms

For a listing of the conditions that trigger Control Board alarms, see "M320 Router Chassis Component Alarm Conditions" on page 74, "T320 Router Chassis Component Alarm Conditions" on page 77, and "T640 Routing Node Chassis Component Alarm Conditions" on page 80.

Table 73 lists the Control Board alarm messages that display on the router craft interface LCD and at the CLI command line for the M320 and T320 routers and the T640 routing node.

Table 73: Control Board Alarm Messages

Component	LCD Short Version	CLI Long Version
Control Board	CB *CB-number* Failure	RED ALARM - CB *CB-number* Failure
	CB *CB-number* Removed	RED ALARM - CB *CB-number* Removed

Action To display any active Control Board alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time              Class  Description
2004-01-07 17:35:03 PST  Major CB 1 Failure
```

What It Means The command output displays the current FPC alarms, including the time the alarm occurred, the severity level, and the alarm description.

Alternative Actions To check for Control Board errors, you can also look at the show chassis craft-interface CLI command output or check the LEDs on the Control Board faceplate.

Step 2: Check the Control Board LEDs

Action To check the Control Board LEDs, look at the three LEDs located on the Control Board faceplate. Figure 124 on page 303, Figure 125 on page 304, and Figure 129 on page 314 show the Control Board faceplates. Table 74 describes the functions of the Control Board LEDs.

NOTE: The online/offline button on the Control Board is currently nonfunctional.

Table 74: Control Board LEDs

Label	Color	State	Description
OK	Green	On steadily	Control Board is online and functioning normally.
FAIL	Amber	On steadily	Control Board has failed.
MASTER	Blue	On steadily	Control Board is functioning as master.

Step 3: Display Control Board Error Messages in the System Log File

Action To check for Control Board error messages in the system log messages file, use the following CLI command:

user@host> **show log messages | match cb**

Check for messages at least 5 minutes before and after a Control Board alarm occurs.

Sample Output

```
user@host> show log messages | match cb
May 18 16:04:06  routerhost chassisd[4836]: CHASSISD_FRU_OFFLINE_NOTICE: CB 1
offline: Offlined
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match cb command to see error messages that are generated when a Control Board fails or is offline. Use this information to diagnose a Control Board problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 4: Display Control Board Error Messages in the Chassis Daemon Log File

Action To display Control Board error messages in the chassisd log file, use the following CLI command:

user@host> **show log chassisd | match cb**

Sample Output

```
user@host> show log chassisd | match cb
May 18 16:04:06 CHASSISD_FRU_OFFLINE_NOTICE: Taking CB 1 offline: Offlined
```

```
May 18 16:04:06 GBUS cmd to CB#1 [0x9], Green LED Off [0x1a]
May 18 16:04:06 CB#1 - Green LED Off
May 18 16:04:06 hwdb: entry for cbd 296 at slot 1 deleted
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the chassisd log file by using the | match cb command to see error messages that are generated when a Control Board fails or is offline. Use this information to diagnose a Control Board problem and to let JTAC know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Verifying Control Board Failure

Steps To Take To verify a Control Board failure, follow these steps:

1. Check the Control Board Connection on page 310
2. Check the Control Board Fuses on page 311
3. Perform a Control Board Swap Test on page 312
4. Display the Control Board Hardware Information on page 313
5. Locate the Control Board Serial Number ID Label on page 314

Step 1: Check the Control Board Connection

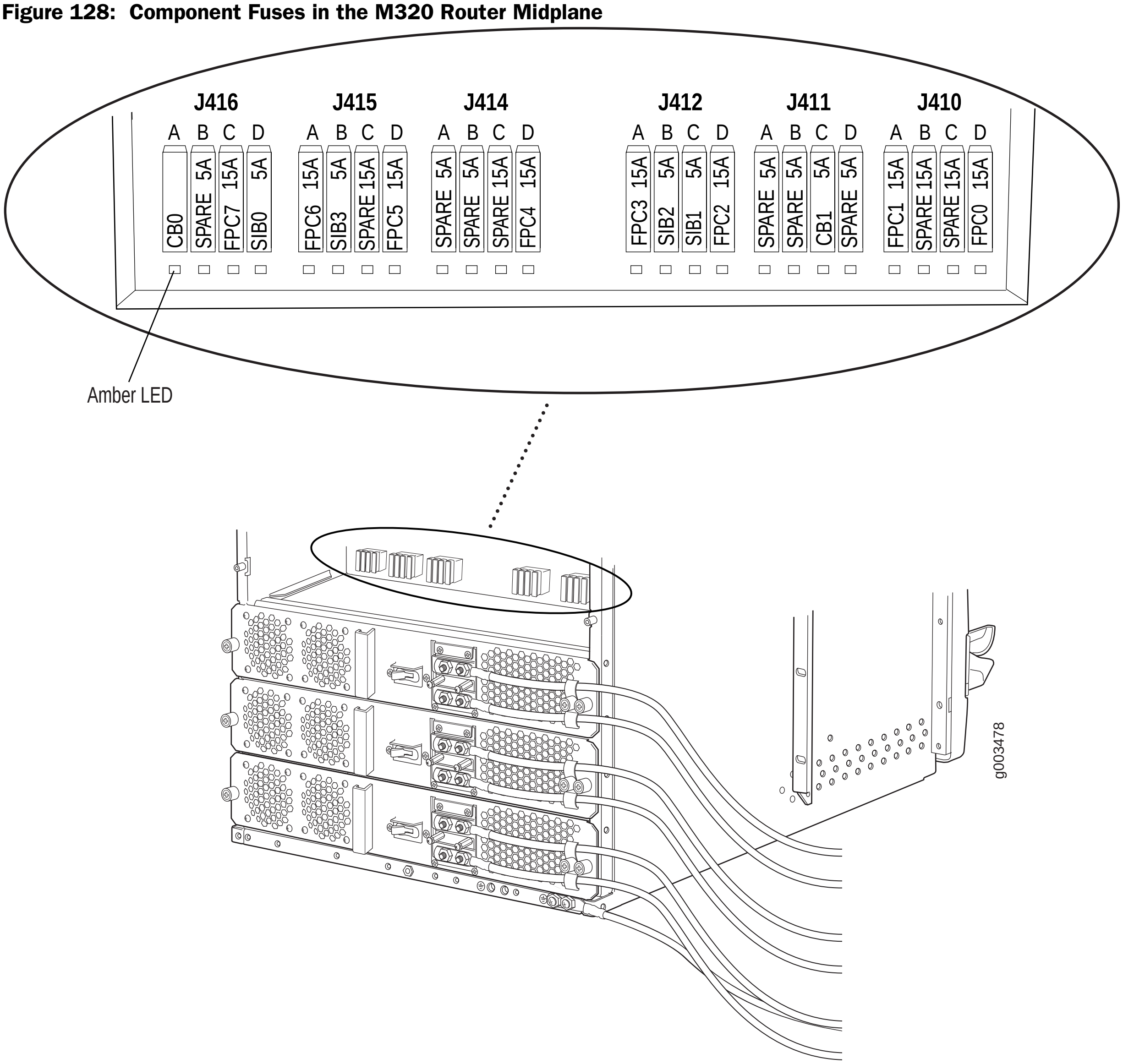
Action To check the Control Board connection, make sure that it is properly seated in the midplane. Ensure that none of the pins are bent. Check the captive screws on the Control Board ejector handles.

Step 2: Check the Control Board Fuses

The M320 router requires fuses for the Control Board. The fuses for the Control Board, Switch Interface Boards (SIBs) and Flexible PIC Concentrators (FPCs) are located in the rear of the midplane behind the power supply in slot PEM0. When the fuse for a Control Board blows, the Control Board stops functioning even though it is installed correctly and the power supplies are providing power to the router.

Figure 128 shows the location of the fuses in the rear of the midplane for the Control Boards. (The labels shown in the figure do not appear on the actual fuses—the clear cover on every fuse reads BUSS GMT-X—and might not match the labels on the midplane. Ignore the labels on the midplane.)

Figure 128: Component Fuses in the M320 Router Midplane



Step 3: Perform a Control Board Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the Conrol Board for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a Control Board swap test, follow these steps:

1. Determine whether the host subsystem is functioning as master or backup, using one of the two following methods:

   - Check the host subsystem LEDs on the craft interface. If the green MASTER LED is lit, the corresponding host subsystem is functioning as master.

   - Display which host subsystem is functioning as master, using the following CLI command:

     user@host> **show chassis routing-engine**

2. If the host subsystem is functioning as master, switch it to backup, using the following CLI command:

   user@host> **request chassis routing-engine master switch**

   When you switch the host subsystem from master to backup, the functioning of the routing node is interrupted for up to several minutes as the system reboots and the new master host subsystem downloads software to the SIBs.

3. Have ready an antistatic mat, placed on a flat, stable surface.

4. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis.

5. Loosen the captive screws on the ejector handles on both sides of the Control Board faceplate.

6. Flip the ejector handles outwards to unseat the Control Board.

7. Grasp the ejector handles and slide the Control Board about halfway out of the chassis.

8. Move one of your hands underneath the Control Board to support it, and slide it completely out of the chassis.

9. Remove the replacement Control Board from its electrostatic bag.

10. Carefully align the sides of the Control Board with the guides inside the chassis.

11. Slide the Control Board all the way into the chassis.

12. Grasp both ejector handles and press them inwards to seat the Control Board.

13. Tighten the captive screws on the ejector handles.

14. To bring the Control Board online, press the online/offline button until the green ONLINE LED lights.

Step 4: Display the Control Board Hardware Information

Action To display the Control Board hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
t640@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                65565             M320
Midplane         REV 05   710-009120   RB0662            M320 Midplane
FPM GBUS         REV 04   710-005928   HV7564            M320 Board
FPM Display      REV 05   710-009351   HY0996            VFPD
CIP              REV 04   710-005926   HV2440            SCP
PEM 0            Rev 03   740-009148   QD17663           DC Power Entry Module
PEM 1            Rev 03   740-009148   QD17664           DC Power Entry Module
PEM 2            Rev 03   740-009148   QD17662           DC Power Entry Module
PEM 3            Rev 03   740-009148   QD16006           DC Power Entry Module
Routing Engine 0 REV 05   740-008883   P11123900322      RE-4.0
Routing Engine 1 REV 05   740-008883   P11123900311      RE-4.0
CB 0             REV 07   710-009115   HW8716            M320 Control Board
CB 1             REV 07   710-009115   HW8693            M320 Control Board
[...Output truncated...]
```

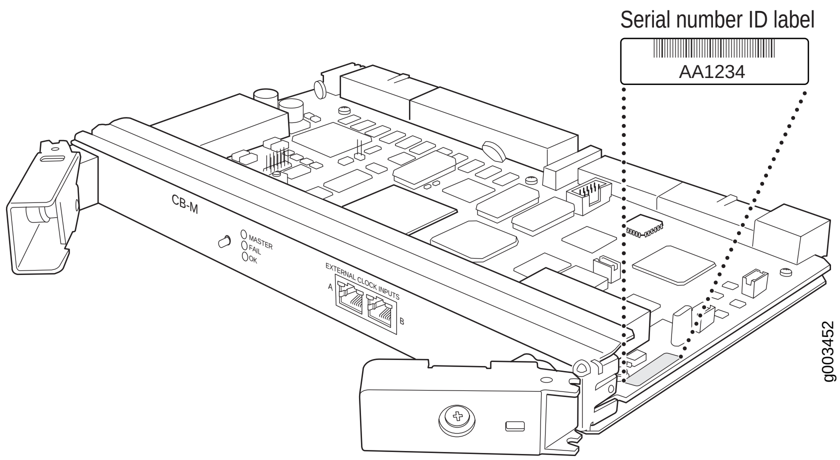
What It Means The command output displays the Control Board slot number, revision level, part number, serial number, and description. The command output for this T640 routing node shows two Control Boards installed in slots CB0 and CB1.

Step 5: Locate the Control Board Serial Number ID Label

Action To find the Control Board serial number ID label locations, do the following:

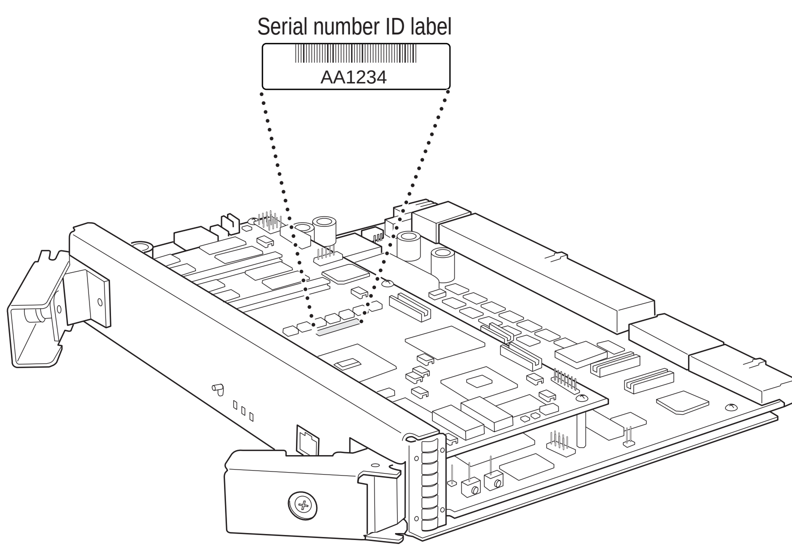
On the M320 router, look on the right side of the top of the Control Board (see Figure 129).

Figure 129: M320 Router Control Board Serial Number ID Label Location



On the T320 router and the T640 routing node, look on the bottom left side of the Control Board (see Figure 130).

Figure 130: T320 Router and T640 Routing Node Control Board Serial Number ID Label



Returning the Control Board

Action To return the Control Board, see "Return the Failed Component" on page 86 or follow the procedure in the appropriate router hardware guide.

Chapter 23

Monitoring the SCGs

You monitor the SONET Clock Generators (SCGs) that provide a clock signal for the SONET/SDH interfaces on the T320 router and the T640 routing node. The SCGs select a clock signal from any Flexible PIC Concentrator (FPC). (See Table 75.)

Table 75: Checklist for Monitoring the SCG

Monitor SCG Tasks	Command or Action
Understanding the SCG on page 316	
Monitoring the SCG Status on page 317	
1. Monitor the SCG Environmental Status on page 317	show chassis environment show chassis environment scg
2. Display the SCG LED States at the Command Line on page 318	show chassis craft-interface
3. Look at the SCG LEDs on the Faceplate on page 319	
Determining SCG Mastership on page 319	
1. Display the SCG Master from the Craft Interface Output on page 319	show chassis craft-interface
2. Look at the SCG LEDs on the Faceplate on page 320	
Displaying SCG Alarms on page 320	
1. Display Current SCG Alarms on page 320	show chassis alarms
2. Display SCG Error Messages in the System Log File on page 321	show log messages
3. Display SCG Error Messages in the Chassis Daemon Log File on page 321	show log chassisd
Verifying SCG Failure on page 322	
1. Check the SCG Connection on page 322	1. Make sure the SCG is properly seated in the midplane. 2. Make sure none of the SCG pins are bent. 3. Check the thumbscrew on the right side of the SCG.
2. Perform an SCG Swap Test on page 322	1. Take the SCG offline. 2. Replace the SCG with one that you know works. 3. Bring the SCG online. 4. Check the SCG status.

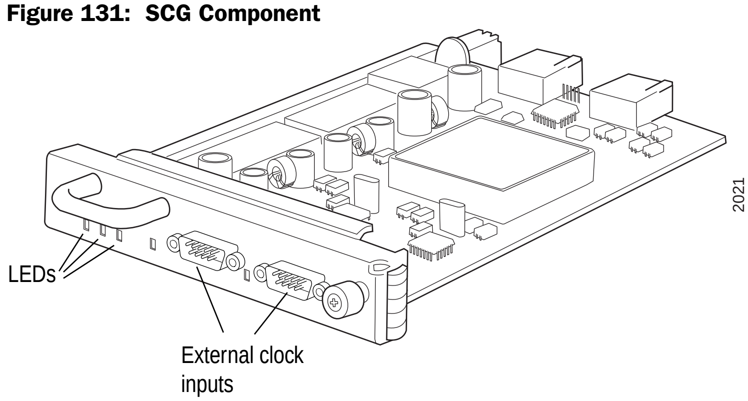
Monitor SCG Tasks	Command or Action
Getting SCG Hardware Information on page 323	
1. Display the SCG Hardware Information on page 323	show chassis hardware
2. Locate the SCG Serial Number ID Label on page 324	Look on the top of the SCG, close to the midplane connector.
Returning the SCG on page 324	See "Return the Failed Component" on page 86, or follow the procedure in the appropriate router hardware guide.

Understanding the SCG

Purpose You monitor the SCGs to ensure that they provide a clock signal for the SONET/SDH interfaces on the router and that they select a clock signal from any FPC, or from the external clock inputs.

What Is an SCG The SCGs provide a 19.44-MHz Stratum 3 clock signal for the SONET/SDH interfaces on the router. The SCGs can also select a clock signal from any FPC, or from the external clock inputs (see Figure 131).

Figure 131: SCG Component



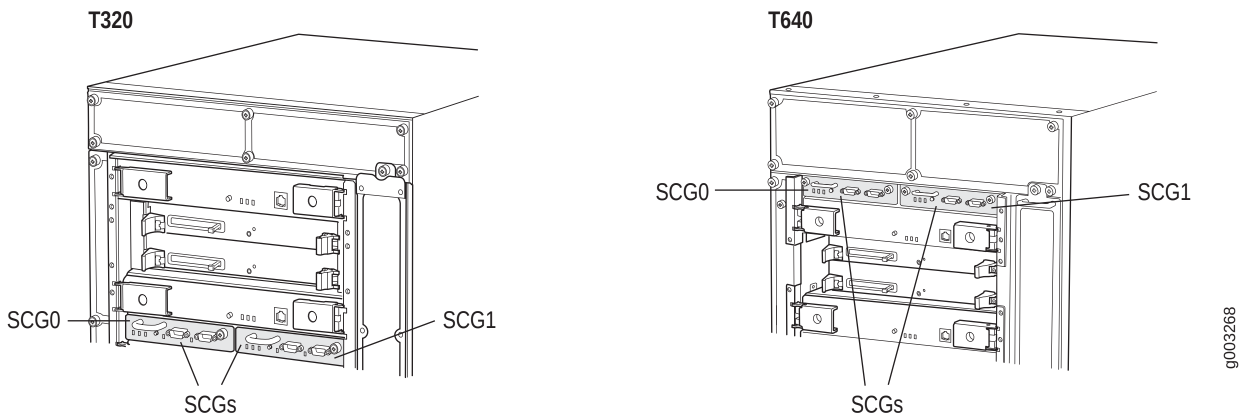
Two SCGs are installed in the T320 router and the T640 routing node. The SCGs install into the upper rear of the chassis in the slots labeled SCG0 and SCG1.

If both SCGs are installed and functioning normally, SCG0 is master and SCG1 is backup. Removing the backup SCG does not affect the functioning of the router or routing node. Taking the master SCG offline might result in a brief loss of SONET clock lock while the backup SCG becomes master.

The SCGs are hot-pluggable.

Figure 132 on page 317 shows the location of the SCGs on the T320 router and T640 routing node.

Figure 132: T320 Router and T640 Routing Node SCG Location



Monitoring the SCG Status

Steps To Take To monitor the SCG status, follow these steps:

1. Monitor the SCG Environmental Status on page 317
2. Display the SCG LED States at the Command Line on page 318
3. Look at the SCG LEDs on the Faceplate on page 319

Step 1: Monitor the SCG Environmental Status

Action To monitor the SCG environment status, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis environment**

Sample Output

```
t320@host> show chassis environment
Class Item                   Status     Measurement
Power PEM 0                  Absent
      PEM 1                  OK
Temp  SCG 0                  OK         30 degrees C / 86 degrees F
      SCG 1                  OK         29 degrees C / 84 degrees F
[...Output truncated...]
```

What It Means The command output displays the status and temperature for each SCG.

Alternative Action If there is a problem with the SCG status, you can display more detailed SCG environmental information with the following CLI command:

user@host> **show chassis environment scg**

The command output is as follows:

```
t320@host> show chassis environment scg
SCG 0 status:
  State                           Online -  Master clock
  Temperature                  30 degrees C / 86 degrees F
  Power:
    GROUND                      0 mV
    3.3 V                    3317 mV
    5.0 V                    5072 mV
    5.6 V                    5697 mV
    1.8 V bias               1794 mV
    3.3 V bias               3304 mV
    5.0 V bias               4991 mV
    8.0 V bias               7318 mV
  BUS Revision                 40
SCG 1 status:
  State                           Online - Standby
  Temperature                  29 degrees C / 84 degrees F
  Power:
    GROUND                      0 mV
    3.3 V                    3318 mV
    5.0 V                    5084 mV
    5.6 V                    5704 mV
    1.8 V bias               1782 mV
    3.3 V bias               3286 mV
    5.0 V bias               5003 mV
    8.0 V bias               7323 mV
  BUS Revision                 40
```

The command output displays the status for each SCG slot 0 and 1. The operating status can be Present, Online, Offline, or Empty. If Online, it can be the clock source (Master clock) or backup (Standby). The command output displays the temperature of the air flowing past the SCG. The command output also displays information about the SCG power supplies and the SCG circuitry revision level.

Step 2: Display the SCG LED States at the Command Line

Action To display the SCG LED states, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
t320@host> show chassis craft-interface
[...Output truncated...]
SCG LEDs:
  SCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .
[...Output truncated...]
```

What It Means The command output displays the SCG LED status. The router has two SCGs installed. Asterisks (*) indicate the operation status. The color represents the possible SCG operating states: Amber (Fail), Green (OK), and Blue (Master). Both SCGs are functioning properly (Green). The SCG in slot 0 is operating as master; the SCG in slot 1 is the backup.

Step 3: Look at the SCG LEDs on the Faceplate

Action To view the SCG LEDs, remove the rear component cover and look on the SCG faceplate at the rear of the router chassis (see Figure 131 on page 316 and Figure 132, “T320 Router and T640 Routing Node SCG Location” on page 317). Table 76 describes the functions of these LEDs.

Table 76: SCG LEDs

Label	Color	State	Description
OK	Green	On steadily	SCG is online and functioning normally.
FAIL	Amber	On steadily	SCG has failed.
MASTER	Blue	On steadily	SCG is functioning as master.

Determining SCG Mastership

If both SCGs are installed and functioning normally, SCG0 is master and SCG1 is backup. Removing the backup SCG does not affect the functioning of the routing node. Taking the master SCG offline might result in a brief loss of SONET clock lock while the backup SCG becomes master.

Steps To Take To determine which SCG is operating as the master, follow these steps:

1. Display the SCG Master from the Craft Interface Output on page 319
2. Look at the SCG LEDs on the Faceplate on page 320

Step 1: Display the SCG Master from the Craft Interface Output

Action To determine the SCG master from the craft interface status information, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
SCG LEDs:
  SCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .
[...Output truncated...]
```

What It Means The command output displays which SCG is operating as master. Asterisks (*) indicate the operation status. The color represents the possible SCG operating states: Amber (Fail), Green (OK), and Blue (Master). The SCG in slot 0 is operating as master; the SCG in slot 1 is the backup.

Step 2: Look at the SCG LEDs on the Faceplate

Action Check the blue MASTER LED on the SCG faceplate. If this LED is on steadily, the SCG is functioning as master. Table 76 describes the functions of these LEDs.

Displaying SCG Alarms

Steps To Take To display SCG alarms and error messages, follow these steps:

1. Display Current SCG Alarms on page 320
2. Display SCG Error Messages in the System Log File on page 321
3. Display SCG Error Messages in the Chassis Daemon Log File on page 321

Step 1: Display Current SCG Alarms

Table 77 describes the SCG alarms that display on the router craft interface LCD display at the CLI command line.

Table 77: SCG Alarm Messages

Component	LCD Short Version	CLI Long Version
SCG	SCG *SCG-number* Failure	RED ALARM—SCG *SCG-number* Failure
	SCG *SCG-number* Removed	RED ALARM—SCG *SCG-number* Failure
	SCG *SCG-number* Not Online	YELLOW ALARM—SCG *SCG-number* Not Online

For the conditions that trigger SCG alarms, see “T320 Router Chassis Component Alarm Conditions” on page 77 and “T640 Routing Node Chassis Component Alarm Conditions” on page 80.

Action To display the current SCG alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
t320@host> show chassis alarms
1 alarm currently active
Alarm time              Class  Description
2004-01-28 14:53:10 PST  Minor  SCG 0 Not Online
```

What It Means The command output displays the alarm date, time, severity level, and description.

Step 2: Display SCG Error Messages in the System Log File

Action To display the SCG error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
t320@host> show log messages | match scg
Jan 28 14:53:10  utah chassisd[2384]: CHASSISD_FRU_OFFLINE_NOTICE: Taking SCG 0
offline - Offlined by cli command
Jan 28 14:53:10  utah craftd[2386]:  Minor alarm set, SCG 0 Not Online
Jan 28 14:53:10  utah alarmd[2385]: Alarm set: SCG color=YELLOW, class=CHASSIS,
reason=SCG 0 Not Online
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match scgs command to see error messages that are generated when an SCG fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display SCG Error Messages in the Chassis Daemon Log File

Action To display the SCG error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
t320@host> show log chassisd
Dec 17 11:11:12 SCG 1 removed
Dec 17 11:11:12 CHASSISD_FRU_OFFLINE_NOTICE: Taking SCG 1 offline - Removal
Dec 17 11:11:12 CHASSISD_SNMP_TRAP7: SNMP trap: FRU removal: jnxFruContentsIndex
11, jnxFruL1Index 2, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName SCG 1,
jnxFruType 2, jnxFruSlot 2
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Verifying SCG Failure

Steps To Take To verify SCG failure, follow these steps:

1. Check the SCG Connection on page 322
2. Perform an SCG Swap Test on page 322

Step 1: Check the SCG Connection

Action To check the SCG connection, make sure the SCG is properly seated in the midplane. Make sure none of the SCG pins are bent. Check the thumbscrew on the right side of the SCG.

Step 2: Perform an SCG Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SCG for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on a SCG, follow these steps:

1. Take the SCG offline by doing one of the following:
   - Use the following CLI command:

     user@host> **request chassis scg offline slot** *number*

   - Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis. Press the online/offline button on the SCG faceplate and hold it down until the LED goes out (about 5 seconds).
2. Loosen the captive screws on the edges of the SCG faceplate.
3. Grasp the SCG by the handle on the faceplate and slide it out of the chassis.
4. Place the SCG on the antistatic mat.
5. Remove the replacement SCG from its electrostatic bag.
6. Carefully align the sides of the SCG with the guides in the SCG slot.
7. Grasp the SCG by its handle and slide it straight into the chassis until it contacts the midplane.
8. Tighten the captive screws on the corners of the SCG faceplate.

9. Bring the SCG online by doing one of the following:
   - Use the following CLI command:

     user@host> r**equest chassis scg online slot** *number*

   - Press the online/offline button until the green ONLINE LED lights.

10. Verify that the SCG is online by using the following CLI command:

    user@host> **request chassis scg online slot** *number*

    If the replaced SCG is online, the removed SCG has failed. Return the SCG as described in “Return the Failed Component” on page 86.

Getting SCG Hardware Information

Steps To Take To get the SCG hardware information, follow these steps:

1. “Display the SCG Hardware Information” on page 323
2. “Locate the SCG Serial Number ID Label” on page 324

Step 1: Display the SCG Hardware Information

Action To display the SCG hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

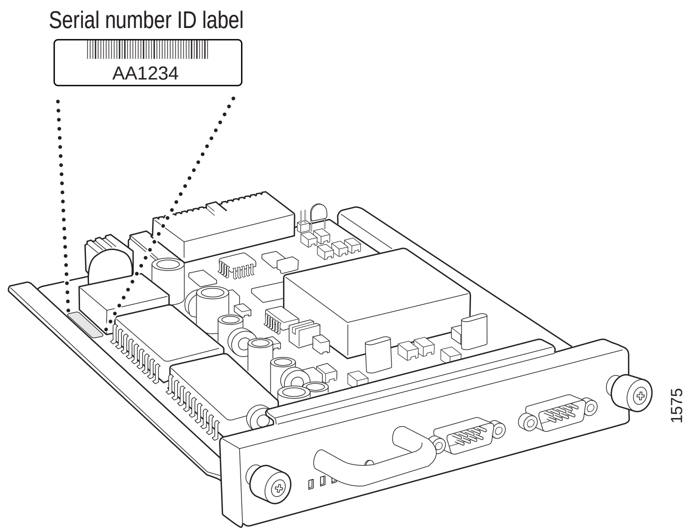
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                abcdef            T320
Midplane         REV 01   710-004339   AY4529
FPM GBUS         REV 02   710-004461   AY4511
FPM Display      REV 02   710-002897   HF6094
CIP              REV 05   710-002895   HC0468
PEM 1            Rev 01   740-004359   2708013           Power Entry Module
SCG 0            REV 06   710-004455   AY4526
SCG 1            REV 06   710-004455   AY4523
```

What It Means The command output displays the SCG slot number, revision level, part number, and serial number.

Step 2: Locate the SCG Serial Number ID Label

Action The serial number is located on the top of the SCG, close to the midplane connector (see Figure 133).

Figure 133: Serial Number Label on the SCG



Returning the SCG

The SCGs are hot-pluggable. If both SCGs are installed and functioning normally, SCG0 is master and SCG1 is backup. Removing the backup SCG does not affect the functioning of the routing node. Taking the master SCG offline might result in a brief loss of SONET clock lock while the backup SCG becomes master.

Action To return an SCG, see the appropriate router hardware guide.

Chapter 24

Monitoring the SIBs

You monitor the Switch Interface Boards (SIBs) that provide the switching function to the destination Flexible PIC Concentrator (FPC). The SIBs create the switch fabric for the routing platforms, providing up to a total of 640 million packets per second (Mpps) of forwarding. (See Table 78.)

Table 78: Checklist for Monitoring the SIBs

Monitor SIB Tasks	Command or Action
Understanding the SIBs on page 326	
■ M320 Router, T320 Router, and T640 Routing Node SIB Location on page 328 ■ M320 Router SIBs on page 329 ■ T320 Router SIBs on page 329 ■ T640 Routing Node SIBs on page 329	
Monitoring the SIB Status on page 329	
1. Display the SIB Summary Status on page 330	show chassis sibs
2. Display the SIB LED Status at the Command Line on page 330	show chassis craft-interface
3. Check the SIB LED Status on the Faceplate on page 330	Check the SIB faceplate at the back of the T320 router and the T640 routing node chassis.
4. Display the SIB Environmental Status on page 331	show chassis environment show chassis environment sib *slot*
Displaying SIB Alarms on page 332	
1. Display Current SIB Alarms on page 332	show chassis alarms
2. Display SIB Error Messages in the System Log File on page 333	show log messages| match sib
3. Display SIB Error Messages in the Chassis Daemon Log File on page 333	show log chassisd | match sib
Verifying SIB Failure on page 334	
1. Check the SIB Connection on page 334	1. Make sure that the SIB is properly seated in the midplane. 2. Ensure that none of the pins are bent. 3. Check the thumbscrews on the ejector locking tabs.
2. Check the SIB Fuses on page 334	The fuses for the SIBs are located in the rear of the midplane behind the power supply in slot PEM0.

Monitor SIB Tasks	Command or Action
3. Perform an SIB Swap Test on page 336	1. Take the SIB offline. 2. Replace the SIB with one that you know works. 3. Bring the SIB online. 4. Check the SIB status.
Getting SIB Hardware Information on page 337	
1. Display SIB Hardware Information on page 337	show chassis hardware
2. Locate the SIB Serial Number ID Label on page 338	Look on the top left of the SIB component.
Returning the SIB on page 338	Follow the procedure in the appropriate router hardware guide.

Understanding the SIBs

Purpose Inspect the SIBs to ensure that they provide the switching function to the destination FPCs.

What Is an SIB A SIB forwards packets to a destination FPC.

Table 79 shows the SIB characteristics for the M320 router, T320 router, and the T640 routing node.

Table 79: SIB Packet Forwarding Characteristics

Routing Platform	Million Packets per Second (Mpps) Forwarding	Number of SIBs per Chassis	Redundancy
M320	385	4	No
T320	320	3	Yes
T640	640	5	Yes

Figure 134 shows the M320 router SIB component.

Figure 134: M320 Router SIB Component

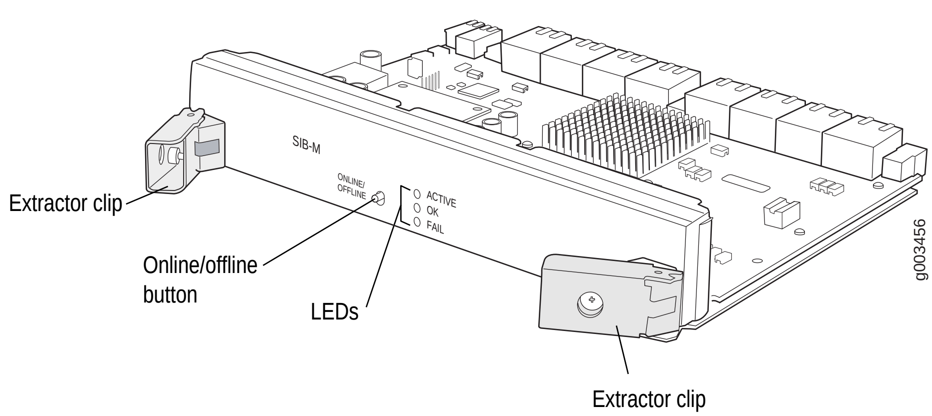


Figure 138 shows the T320 router and T640 routing node SIB component.

Figure 135: T320 Router and T640 Routing Node SIB Component

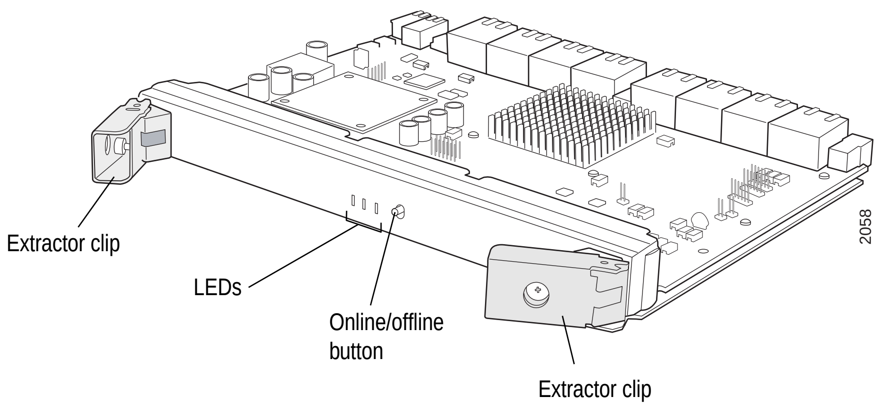
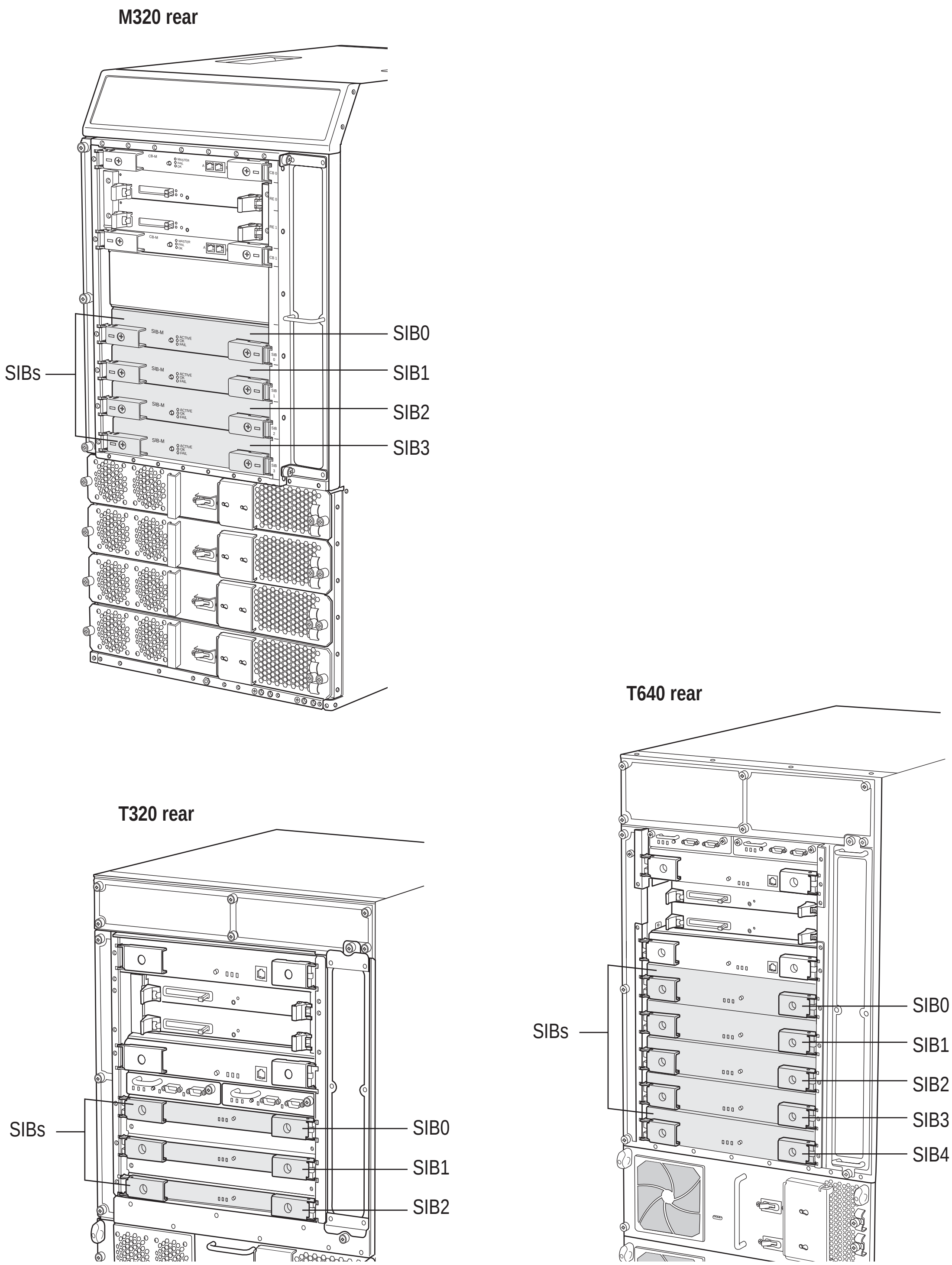


Figure 136 shows the location of the SIBs on the M320 router, T320 router, and the T640 routing node.

Figure 136: M320 Router, T320 Router, and T640 Routing Node SIB Location



M320 Router SIBs

Four SIBs are installed in the M320 router. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB3 (top to bottom). See Figure 136 on page 328. All four SIBs are active, and there is no backup.

T320 Router SIBs

Three SIBs are installed in the router. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB2 (see Figure 136 on page 328).

Each FPC has a dedicated ASIC with five high-speed links that connect to the SIBs. Two high-speed links connect to SIB1 and SIB2. One high-speed link connects to SIB0. SIB0 acts as a backup to SIB1 and SIB2. In the event of a complete SIB failure, SIB0 will become active. Because SIB0 has only one high-speed link to each FPC, only three links will remain active. A slight degradation in forwarding capacity may occur. When the failed SIB is replaced, it will become active and SIB0 will revert to backup. The router will regain full forwarding capacity.

T640 Routing Node SIBs

Five SIBs are installed in the routing node. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB4 (top to bottom). See Figure 136 on page 328.

Each FPC1 and FPC2 has a dedicated ASIC with five high-speed links that connect to the SIBs (one link per SIB). An FPC3 has two dedicated ASICs, and each ASIC has five high-speed links that connect to the SIBs (a total of 10 links). One of the five SIBs—usually SIB4—acts as a backup to the remaining four SIBs. In the event of a SIB failure, the backup SIB becomes active and traffic forwarding continues without any degradation. When the failed SIB is replaced, it becomes the new backup.

Monitoring the SIB Status

Steps To Take To monitor the SIB status, follow these steps:

1. Display the SIB Summary Status on page 330
2. Display the SIB LED Status at the Command Line on page 330
3. Check the SIB LED Status on the Faceplate on page 330
4. Display the SIB Environmental Status on page 331

Step 1: Display the SIB Summary Status

Action To display the SIB summary status, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis sibs**

Sample Output

```
t640@host> show chassis sibs
Slot  State              Uptime
 0    Spare
 1    Online            4 hours, 5 minutes, 47 seconds
 2    Online            4 hours, 5 minutes, 42 seconds
 3    Online            4 hours, 5 minutes, 37 seconds
 4    Online            4 hours, 5 minutes, 33 seconds
```

What it Means The command output displays the SIB slot number: 0, 1, 2, 3, and 4. The output also displays the operating status of each SIB as Online, Offline, or Empty, and how long each SIB has been online.

Step 2: Display the SIB LED Status at the Command Line

Action To display the SIB LED status, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
t640@host> show chassis craft-interface
[...Output truncated...]
SIB LEDs:
  SIB  0   1   2   3   4
--------------------------
Red    .   .   .   .   .
Green  *   *   *   *   *
```

What it Means The command output is for a T640 routing node. Asterisks (*) represent the operating state. The status colors represent the possible SIB operating states: Red (Fail) and Green (OK). All SIBs are functioning normally.

Step 3: Check the SIB LED Status on the Faceplate

Action To check the SIB LED status, remove the component cover and look on the SIB faceplate at the back of the T320 router and the T640 routing node (see Figure 135 on page 327).

Table 80 describes the SIB LED states.

Table 80: SIB LEDs

Label	Color	State	Description
OK	Green	On steadily	SIB is functioning normally.
		Blinking	SIB is starting up.
FAIL	Amber	On steadily	SIB has failed.
ACTIVE	Green	On steadily	SIB is in active mode.

Step 4: Display the SIB Environmental Status

Action To display the SIB environmental information, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
T640@host> show chassis environment
Class Item                  Status     Measurement
Temp  PEM 0                 Absent
      PEM 1                 OK         32 degrees C / 89 degrees F
      SCG 0                 OK         37 degrees C / 98 degrees F
      SCG 1                 Absent
      Routing Engine 0      OK         35 degrees C / 95 degrees F
      Routing Engine 1      Absent
      CB 0                  OK         36 degrees C / 96 degrees F
      SIB 0                 OK         44 degrees C / 111 degrees F
      SIB 1                 OK         50 degrees C / 122 degrees F
      SIB 2                 OK         50 degrees C / 122 degrees F
      SIB 3                 OK         50 degrees C / 122 degrees F
      SIB 4                 OK         52 degrees C / 125 degrees F
[...Output truncated...]
```

What it Means The command output displays each component installed in the router, including the operating status and temperature.

Alternative Action If there is a problem with the SIB status, you can display more detailed environmental information with the following CLI command:

user@host> **show chassis environment sib**

```
user@host> show chassis environment sib
SIB 0 status:
  State                          Spare
  Temperature                 44 degrees C / 111 degrees F
  Power:
    GROUND                     0 mV
    1.8 V                   1807 mV
    2.5 V                   2478 mV
    3.3 V                   3308 mV
    1.8 V bias              1797 mV
    3.3 V bias              3284 mV
    5.0 V bias              5018 mV
    8.0 V bias              7440 mV
SIB 1 status:
  State                          Online
  Temperature                 50 degrees C / 122 degrees F
  Power:
    GROUND                     0 mV
    1.8 V                   1814 mV
    2.5 V                   2485 mV
    3.3 V                   3321 mV
    1.8 V bias              1794 mV
    3.3 V bias              3313 mV
    5.0 V bias              5028 mV
    8.0 V bias              7553 mV
SIB 2 status:
  [...Output truncated...]
SIB 3 status:
  [...Output truncated...]
SIB 4 status:
  [...Output truncated...]
```

The command output displays the SIB slot, status, and temperature of the air flowing past the SPP card and the power supply voltages.

You can display the environmental status of a particular SIB with the following CLI command:

user@host> **show chassis environment sib** *slot*

Displaying SIB Alarms

Steps To Take To display SIB alarms and error messages, follow these steps:

1. Display Current SIB Alarms on page 332
2. Display SIB Error Messages in the System Log File on page 333
3. Display SIB Error Messages in the Chassis Daemon Log File on page 333

Step 1: Display Current SIB Alarms

Table 81 lists the SIB alarms that display in the craft interface LCD display and at the CLI command line.

For conditions that trigger SIB alarms, see "T320 Router Chassis Component Alarm Conditions" on page 77 and "T640 Routing Node Chassis Component Alarm Conditions" on page 80.

Table 81: SIB Alarm Messages

Component	LCD Short Version	CLI Long Version
SIB	SIB *sib-number* Failure	RED ALARM—SIB *sib-number* Fault
	SIB *sib-number* Removed	RED ALARM—SIB *sib-number* Absent
	Spare SIB Failure	YELLOW ALARM—Spare SIB Fault
	Spare SIB Removed	YELLOW ALARM—Spare SIB Absent
	Check SIB	YELLOW ALARM—Check SIB

Action To display the current SIB alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1alarms currently active
Alarm time              Class  Description
2004-01-29 18:37:09 PST  Minor  SIB 2 Not Online
```

What it Means The command output displays the alarm date, time, severity level, and description.

Step 2: Display SIB Error Messages in the System Log File

Action To display the SIB error messages in the system log file, use the following CLI command:

user@host> **show log messages | match sib**

Sample Output

```
user@host> show log messages | match sib
Jan 29 18:37:07  toto spmb0 CMGSIB: SIB #2 state transition SIB_STATE_ONLINE ->
SIB_STATE_OFFLINE_ACK_WAIT
Jan 29 18:37:09  toto spmb0 CMGSIB: SIB #2 state transition SIB_STATE_OFFLINE_AC
K_WAIT -> SIB_STATE_OFFLINE
Jan 29 18:37:09  toto spmb0 CMGSIB: SIB #0 state transition SIB_STATE_SPARE -> S
IB_STATE_ONLINE_WAIT
```

What it Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match sib command to see error messages that are generated when an SIB fails or is offline. Use this information to diagnose an SIB problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display SIB Error Messages in the Chassis Daemon Log File

The chassis daemon (chassisd) log file keeps track of the state of each chassis component.

Action To display the SIB error messages logged in the chassis daemon log file, use the following CLI command:

user@host> **show log chassisd | match sib**

Sample Output

```
user@host> show log chassisd | match sib
Jan 29 18:37:07 CHASSISD_FRU_OFFLINE_NOTICE: Taking SIB 2 offline - Offlined by
cli command
Jan 29 18:37:07 CHASSISD_SNMP_TRAP10: SNMP trap: FRU power off: jnxFruContentsIn
dex 15, jnxFruL1Index 3, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName SIB 2, jnx
FruType 9, jnxFruSlot 3, jnxFruOfflineReason 7, jnxFruLastPowerOff 1701082, jnxF
ruLastPowerOn 3250
Jan 29 18:37:09 send: yellow alarm set, device SIB 2, reason SIB 2 Not Online
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack plane case. Checking plane control to
all line cards?
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack: Awaiting spmb ack for LC#0!
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack plane case. Checking plane control to
all line cards?
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack: Awaiting spmb ack for LC#0!
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack plane case. Checking plane control to
all line cards?
Jan 29 18:37:09 fm_recv_hsl_start_sib_ack plane case. Sending plane control to a
ll line cards!
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the chassisd log file by using the | match sib command to see error messages that are generated when an SIB fails or is offline. Use this information to diagnose an SIB problem and to let JTAC know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Verifying SIB Failure

Steps To Take To verify SIB failure, follow these steps:

1. Check the SIB Connection on page 334
2. Check the SIB Fuses on page 334
3. Perform an SIB Swap Test on page 336

Step 1: Check the SIB Connection

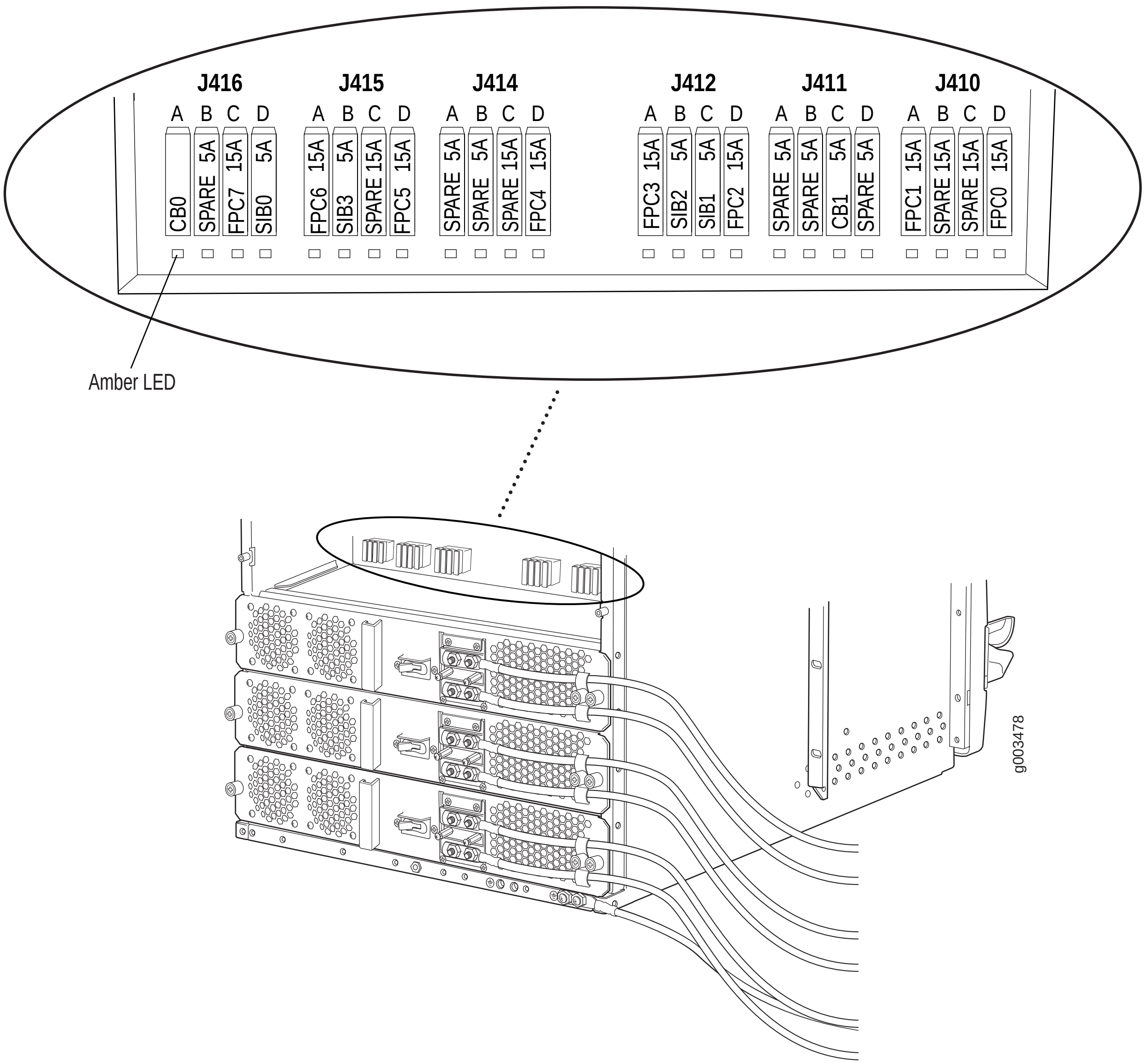
Action To check the SIB connection, make sure that it is properly seated in the midplane. Ensure that none of the pins are bent. Check the thumbscrews on the ejector locking tabs.

Step 2: Check the SIB Fuses

The M320 router requires fuses for the SIBs. The fuses for the Control Board, SIBs, and FPCs are located in the rear of the midplane behind the power supply in slot PEM0. When the fuse for an SIB blows, the SIB stops functioning even though it is installed correctly and the power supplies are providing power to the router.

Figure 137 shows the location of the fuses in the rear of the midplane for the SIBs. (The labels shown in the figure do not appear on the actual fuses—the clear cover on every fuse reads BUSS GMT-X—and might not match the labels on the midplane. Ignore the labels on the midplane.)

Figure 137: Component Fuses in the M320 Router Midplane



Step 3: Perform an SIB Swap Test

SIBs are hot-insertable and hot-removable.

NOTE: Before performing a swap test, always check for bent pins in the midplane and check the SIB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an SIB, follow these steps:

1. Take the SIB offline by doing one of the following

   - Use the following CLI command:

     user@host> **request chassis sib** *slot number* **offline**

   - Press the online/offline button on the SIB faceplate. Press and hold down the button until the green ONLINE LED goes out (about 5 seconds).

2. Have ready an antistatic mat placed on a stable, flat surface.
3. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis.
4. Loosen the captive screws on the ejector handles on each side of the SIB faceplate.
5. Flip the ejector handles outward to unseat the SIB.
6. Grasp both ejector handles, pull firmly on the SIB, and slide the SIB about three-quarters of the way out of the chassis.
7. Move one of your hands underneath the SIB to support it, and slide it completely out of the chassis.
8. Hold the replacement SIB by placing one hand underneath to support it and the other hand on one of the ejector handles on the SIB faceplate.
9. Carefully align the sides of the SIB with the guides inside the chassis.
10. Slide the unit into the chassis, carefully ensuring that it is correctly aligned.
11. Grasp both ejector handles and press them inwards to seat the SIB.
12. Tighten the captive screws on the ejector handles.
13. Bring the SIB online by doing one of the following

    - Use the following CLI command:

      user@host> **request chassis sib** *slot number* **online**

    - Press the offline/online button until the green ONLINE LED lights to bring the SIB online.

Getting SIB Hardware Information

Steps To Take To get the hardware information you need to return a failed SIB, follow these steps:

1. Display SIB Hardware Information on page 337
2. Locate the SIB Serial Number ID Label on page 338

Step 1: Display SIB Hardware Information

Action To display the SIB hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                19061             T640
[...Output truncated...]
SIB 0            REV 05   710-003980   HF9603            SIB-I8
SIB 1            REV 05   710-003980   HF9577            SIB-I8
SIB 2            REV 05   710-003980   HF9540            SIB-I8
SIB 3            REV 05   710-003980   HF9550            SIB-I8
SIB 4            REV 05   710-003980   HF9592            SIB-I8
```

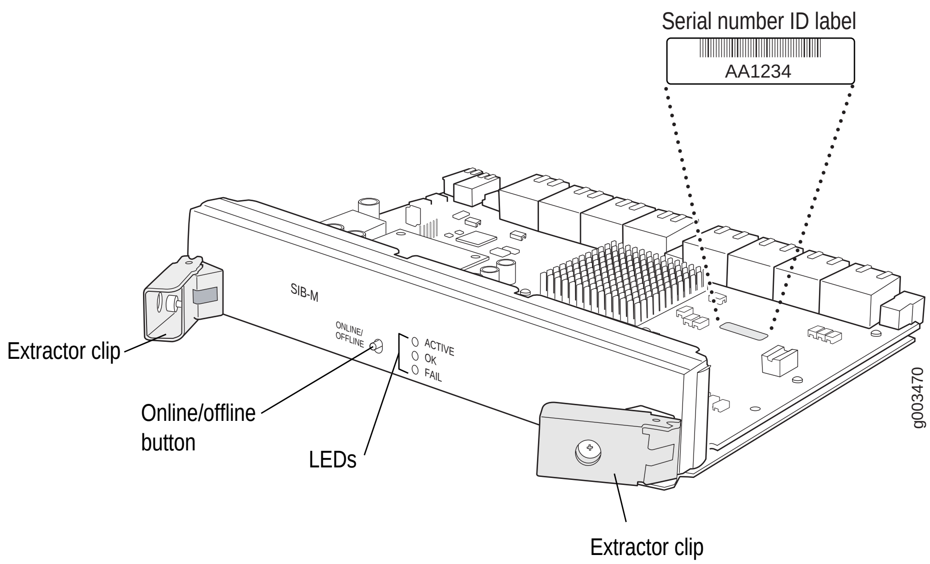
What it Means The command output displays the SIB slot number, revision level, part number, serial number, and description.

Step 2: Locate the SIB Serial Number ID Label

Action To find the SIB serial number ID label locations, do the following:

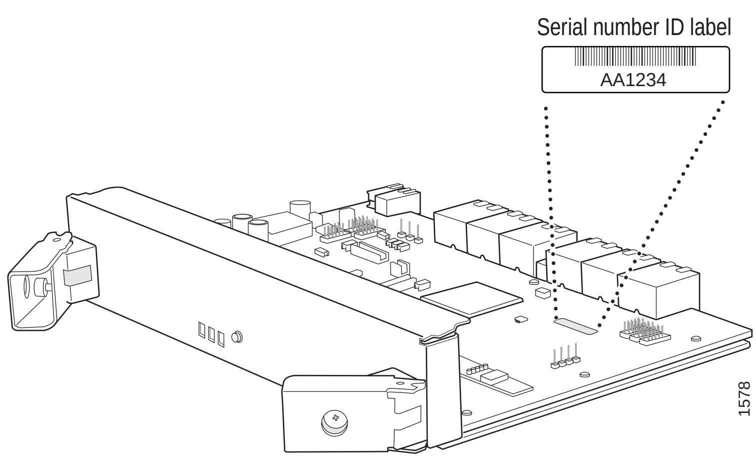
On the M320 router, the SIB serial number label is located on the right side of the top of the component (see Figure 138).

Figure 138: M320 Router SIB Serial Number ID Label location



On the T320 router and the T640 routing node, the SIB serial number ID label is located on the left side of the top panel of the component (see Figure 139).

Figure 139: Serial Number Label on the SIB



Returning the SIB

Action To return a failed SIB, see "Return the Failed Component" on page 86 or the appropriate router hardware guide.

Part 5

Monitoring M40e and M160 Internet Router-Specific Components

Chapter 25

Monitoring the Host Module

You monitor and maintain the M40e and M160 router host module—the Routing Engine and the Miscellaneous Control Subsystem (MCS)—which constructs routing tables, performs system management functions, and generates the SONET/SDH clock signal for SONET/SDH interfaces. (See Table 82.)

Table 82: Checklist for Monitoring the Host Module

Monitor Host Module Tasks	Command or Action
Understanding the Host Module on page 341	
Checking the Host Module Status on page 344	show chassis craft-interface
Checking the Routing Engine Status on page 345	show chassis routing-engine
Checking the MCS Status on page 346	show chassis environment mcs

Understanding the Host Module

Purpose

Inspect the host module to ensure that the Routing Engine and Miscellaneous Control Subsystem (MCS) function properly.

What Is a Host Module

The host module is present on M40e and M160 routers. The host module constructs routing tables, performs system management functions, and generates the SONET/SDH clock signal for SONET/SDH interfaces.

The host module is comprised of two components: the Routing Engine and the MCS. For a host module to function, both of these components must be installed and operational.

Figure 140 shows the Routing Engine component of the host module.

Figure 140: Routing Engine Component

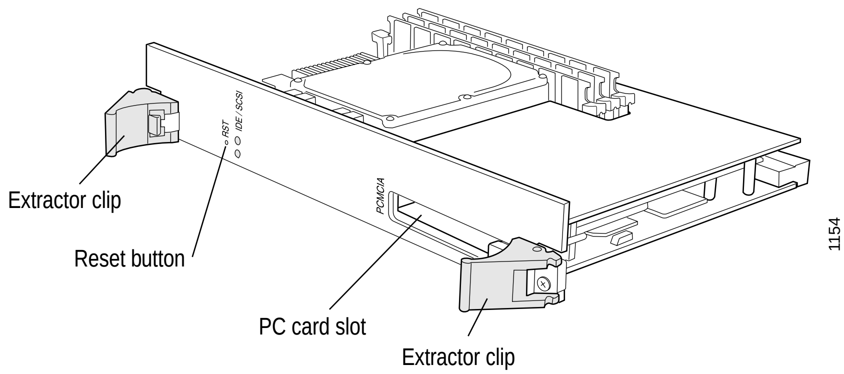
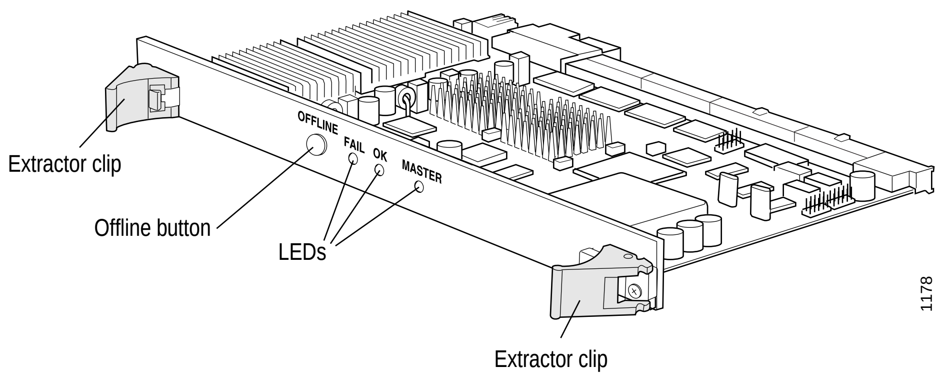


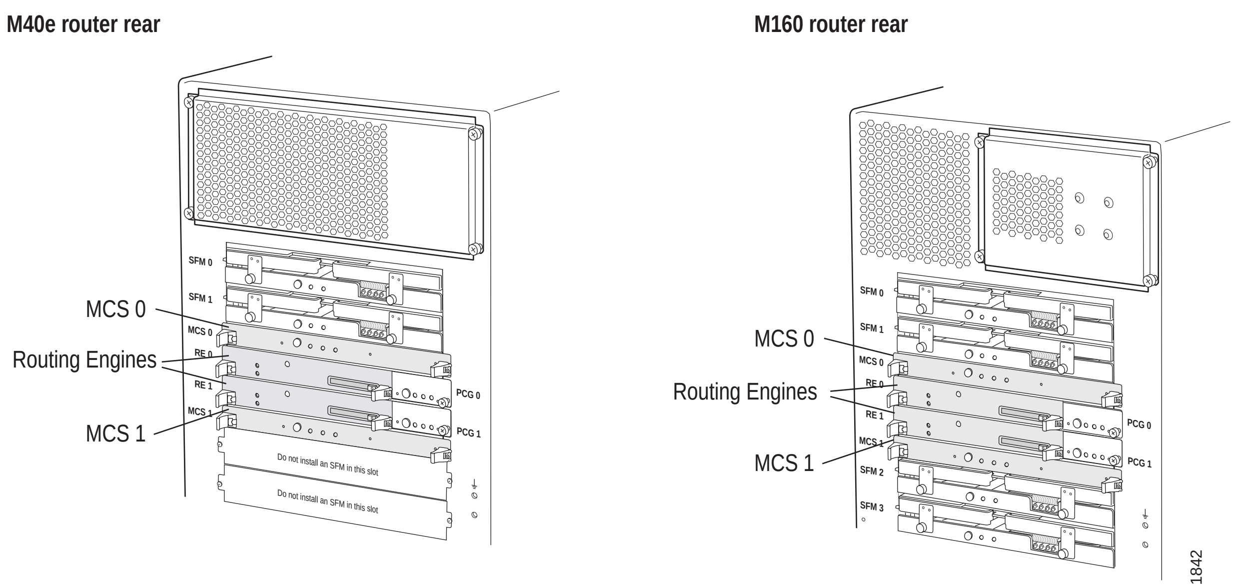
Figure 141 shows the MCS component of the host module.

Figure 141: MCS Component



One or two host modules can be installed into the midplane from the rear of the chassis (see Figure 142). The Routing Engine (slot RE0) is below the MCS slot (MCS0), while slot RE1 is above the MCS1 slot. RE0 must use MCS0 and RE1 must use MCS1 or the circuit will not be connected.

Figure 142: M40e and M160 Router Host Module Location



This chapter provides basic information about monitoring the Routing Engine and the MCS. For more detailed information about monitoring the Routing Engine, see “Monitoring the Routing Engine” on page 125. For more detailed information about monitoring the MCS, see “Monitoring the MCS” on page 359.

See Also

- Monitoring the Host Module on page 341
- Monitoring the MCS on page 359
- Monitoring Redundant Routing Engines on page 491
- Monitoring Redundant MCSs on page 567

Checking the Host Module Status

Action To check the host module status, use the following JUNOS software command-line interface (CLI) operational mode command:

user@host> **show chassis craft-interface**

Output

```
user@host> show chassis craft-interface
[...Output truncated...]
Front Panel System LEDs:
Host     0    1
------------------------
OK       *    .
Fail     .    .
Master   *    .

[...Output truncated...]
```

What It Means (M40e and M160 routers) The Front Panel System LEDs show the Routing Engine Host 0 and Host 1 LED state. The state can be OK, Fail, or Master. An asterisk (*) indicates the operating state.

Alternative Action Look at the LEDs on the craft interface.

The host module LEDs are located on the upper right corner of the craft interface. Two sets of LEDs indicate the host module status: the set labeled HOST0 reports the status of the Routing Engine in slot RE0 and the MCS in slot MCS0, while the set labeled HOST1 reports the status of the Routing Engine in slot RE1 and the MCS in slot MCS1. Each set includes three LEDs: MASTER (green), ONLINE (green), and OFFLINE (red).

Figure 143 shows the M40e and M160 router craft interface LEDs.

Figure 143: M40e and M160 Router Host Module LEDs on the Craft Interface

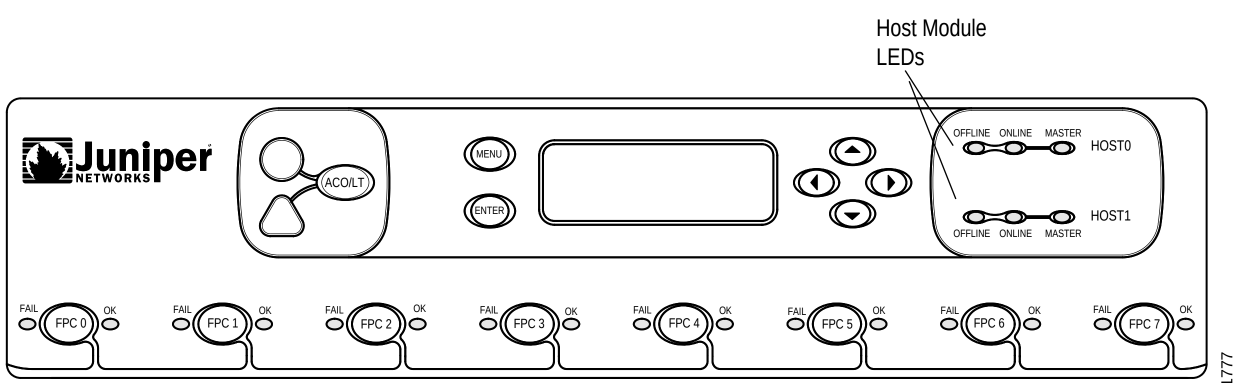


Table 83 describes the M40e and M160 router host module LED states.

Table 83: M40e and M160 Router Host Module LEDs

Label	Color	State	Description
MASTER	Green	On steadily	Host module is functioning as master.
ONLINE	Green	On steadily	Host module components (Routing Engine and MCS) are installed and functioning normally.
		Blinking	Host module is starting up.
OFFLINE	Red	On steadily	One or both host module components are not installed or have failed.

Checking the Routing Engine Status

This section provides a brief description of monitoring the Routing Engines as part of the host module on M40e and M160 routers. For more detailed information about monitoring the Routing Engine, see "Monitoring the Routing Engine" on page 125.

Action To check the Routing Engine status, use the following CLI command:

user@host> **show chassis routing-engine**

Output

```
user@host> show chassis routing-engine
Routing Engine status:
    Temperature                22 degrees C / 71 degrees F
    DRAM                      768 Mbytes
    CPU utilization:
      User                      0 percent
      Background                0 percent
      Kernel                    0 percent
      Interrupt                 0 percent
      Idle                    100 percent
    Model                         teknor
    Serial ID                     4d0000062b049501
    Start time                    2002-04-29 11:18:31 PDT
    Uptime                        5 hours, 20 minutes, 17 seconds
    Load averages:                1 minute   5 minute  15 minute
                                      0.06       0.03       0.00
```

What It Means The command output displays the Routing Engine slot number, current state (Master, Backup, or Disabled), election priority (Master or Backup), and the airflow temperature. The command output also displays the total DRAM available to the Routing Engine processor, the CPU utilization percentage, and the Routing Engine serial number for the slot. Additionally, the command output displays when the Routing Engine started running, how long the Routing Engine has been running, and the time, uptime, and load averages for the last 1, 5, and 15 minutes.

Check the Uptime to ensure that the Routing Engine has not rebooted since it started running.

Checking the MCS Status

This section provides a brief description of monitoring the MCS as part of the host module on M40e and M160 routers. For a more information about monitoring the MCS, see "Monitoring the MCS" on page 359.

Action To monitor the MCS status, use the following CLI command:

user@host> **show chassis environment mcs**

Output

```
user@host> show chassis environment mcs
MCS 0 status:
  State                           Online Master
  Temperature                  43 degrees C / 109 degrees F
  Power:
    3.3 V                    3318 mV
    5.0 V                    4974 mV
    12.0 V                  11824 mV
    5.0 V bias               4974 mV
    8.0 V bias               8212 mV
  BUS Revision                 12
  FPGA Revision                13
MCS 1 status:
  State                           Online Standby
  Temperature                  58 degrees C / 136 degrees F
  Power:
    3.3 V                    3317 mV
    5.0 V                    5006 mV
    12.0 V                  11843 mV
    5.0 V bias               4998 mV
    8.0 V bias               8195 mV
  BUS Revision                 12
  FPGA Revision               255
```

What It Means The show chassis environment mcs CLI command is available on the M40e and M160 routers only. The command output displays environmental information about both MCSs installed in the router or about an individual MCS. It displays the MCS status: Present, Online, Offline, or Empty. The command also indicates whether the MCS is master. The command output displays the temperature of the air flowing past the MCS, information about MCS power supplies, field programmable gate array (FPGA) revision information, and the revision level of the chassis management bus (CMB) slave.

Chapter 26

Monitoring the SFMs

You monitor the Switching and Forwarding Modules (SFMs) to ensure that traffic transiting the router is handled properly. (See Table 84.)

Table 84: Checklist for Monitoring the SFMs

Monitor SFM Tasks	Command or Action
Understanding the SFMs on page 348	
Monitoring the SFM Status on page 349	
1. Display the SFM Summary Status on page 349	show chassis sfm *sfm-slot* show chassis sfm detail *sfm-slot*
2. Display the SFM LED Status at the Command Line on page 351	show chassis craft-interface
3. Check the SFM LED Status on the Faceplate on page 351	Check the SFM faceplate at the back of the M40e and M160 router chassis.
4. Display the SFM Environmental Status on page 351	show chassis environment show chassis environment sfm *sfm-slot*
Displaying SFM Alarms on page 353	
1. Display Current SFM Alarms on page 353	show chassis alarms
2. Display SFM Error Messages in the System Log File on page 353	show log messages
3. Display SFM Error Messages in the Chassis Daemon Log File on page 354	show log chassisd
Verifying SFM Failure on page 355	
1. Check the SFM Connection on page 355	Check the thumbscrews on the SFM ejector locking tabs.
2. Check the SFM Fuses on page 355	The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly.
3. Perform an SFM Swap Test on page 356	1. Take the SFM offline. 2. Replace the SFM with one that you know works. 3. Bring the SFM online. 4. Check the SFM status.
Getting SFM Hardware Information on page 357	
1. Display SFM Hardware Information on page 357	show chassis hardware

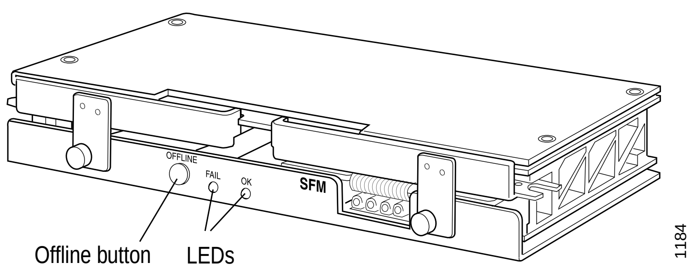
Monitor SFM Tasks	Command or Action
2. Locate the SFM Serial Number ID Label on page 357	Look on the top left of the SFM component.
Replacing the SFM on page 358	See “Return the Failed Component” on page 86, or follow the procedure in the appropriate router hardware guide.

Understanding the SFMs

Purpose Inspect the SFMs to ensure that all traffic leaving the Flexible PIC Concentrators (FPCs) is handled properly.

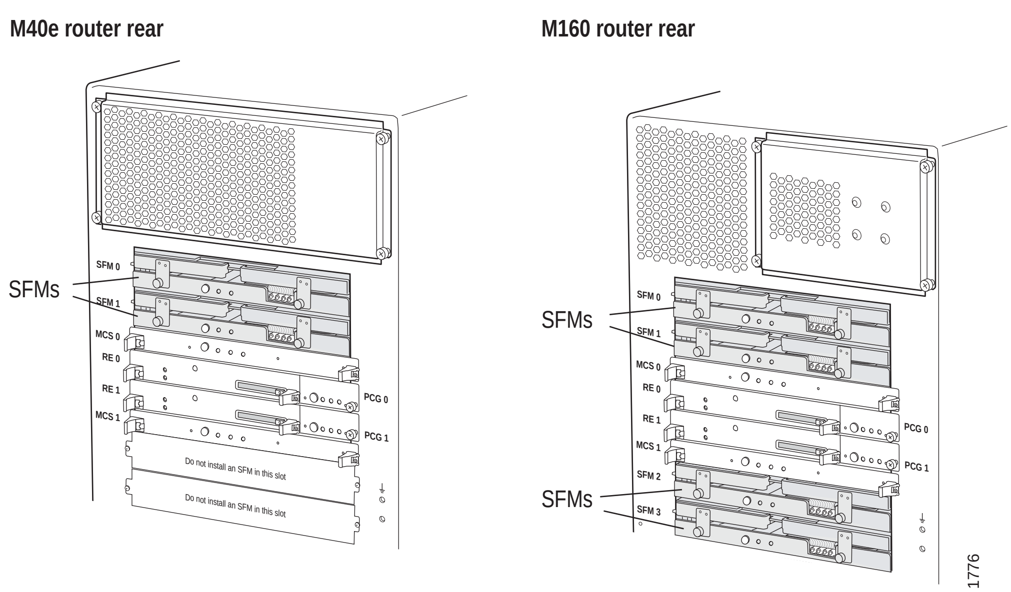
What Is an SFM The SFM is a control board that handles traffic transiting the router (see Figure 144). There are two SFMs on the M40e router and four SFMs on the M160 router (see Figure 145).

Figure 144: SFM Component



The SFMs provide route lookup, filtering, and switching. When the serial stream of bits leaves the FPC, it is directed to one of the SFMs. Each SFM effectively handles one-half or one-quarter of the traffic on each FPC. The SFMs handle a total of 160 million packets per second (Mpps) of forwarding.

Figure 145: M40e and M160 Router SFM Location



The SFMs are hot-removable and hot-insertable. Inserting or removing an SFM causes a brief interruption in forwarding performance (about 500 ms) as the Packet Forwarding Engine reconfigures the distribution of packets across the remaining SFMs.

Monitoring the SFM Status

To monitor the SFM status, follow these steps:

Steps To Take

1. Display the SFM Summary Status on page 349
2. Display the SFM LED Status at the Command Line on page 351
3. Check the SFM LED Status on the Faceplate on page 351
4. Display the SFM Environmental Status on page 351

Step 1: Display the SFM Summary Status

Action To display the SFM summary status, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis sfm**

Sample Output

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           41      2          0        64        16         46
  1  Offline            --- Hard FPC error ---
  2  Online           43      2          0        64        16         46
  3  Online           44      2          0       128         7         46
```

What it Means The command output displays the SFM slot number: 0, 1, 2, or 3. The output also displays the operating status of each SFM as Online, Offline, or Empty.

In the sample output, the root cause of the SFM1 failure may be an FPC problem.

The command output displays the temperature of air passing by the SFM, in degrees Centigrade. It displays the SFM CPU usage, including the total percentage used by the SFM processor and the percentage used for interrupts.

The command output also displays the percentage of memory usage, including the total DRAM available to the SFM processor, in megabytes (MB), and the percentage of heap space (dynamic memory) being used by the SFM processor. Heap utilization greater than 80 percent can indicate a software problem (memory leak). The output shows the percentage of buffer space being used by the SFM processor for buffering internal messages.

Alternative Action If the SFM summary command output indicates that there is a problem, you can display more detailed SFM status information with the following CLI command:

user@host> **show chassis sfm detail**

The command output displays the following information:

Sample Output user@host> **show chassis sfm detail**

```
SFM status:
Slot 0 information:
  State                          Online
  SPP Temperature             36 degrees C / 96 degrees F
  SPR Temperature             45 degrees C / 113 degrees F
  Total CPU DRAM              64 Mbytes
  Total SRAM                   4 Mbytes
  Internet Processor I           Version 1, Foundry IBM, Part number 3
  Start time:                    2001-12-03 05:08:45 PST
  Uptime:                        6 hours, 41 minutes, 17 seconds
Slot 1 information:
  [...Output truncated...]
Slot 2 information:
  [...Output truncated...]
Slot 3 information:
  [...Output truncated...]

Packet scheduling mode: Disabled
```

What It Means In addition to the command output displayed for the show chassis sfm command, the show chassis sfm detail command displays the temperature of air passing by the Switch Plane Processor (SPP) card and the Switch Plane Router (SPR) card (the two SFM serial components) in degrees Centigrade. The command output displays the total CPU DRAM and SRAM being used by the SFM processor. It also displays the time when the SFM became active and how long the SFM has been up and running. A small uptime means that the SFM came online a short time ago and could indicate a possible SFM error condition.

Alternative Action To display the status of a particular SFM, use the following CLI command:

user@host> **show chassis sfm** *sfm-slot*

Alternative Action To display detailed status information about a particular SFM, use the following CLI command:

user@host> **show chassis sfm detail** *sfm-slot*

Step 2: Display the SFM LED Status at the Command Line

Action To display the SFM LED status, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
SFM LEDs:
  SFM  0   1   2   3
-----------------------
Amber  .   .   *   .
Green  *   *   .   *
Blue   *   *   .   *
```

What it Means The command output is for an M160 router. The SFMs in slots 0 and 1 are online and are functioning normally. The status colors represent the possible SFM operating states: Amber (Fail), Green (OK), and Blue (Master). The (*) indicates the current operating state. There are no SFMs in slots 2 and 3.

Step 3: Check the SFM LED Status on the Faceplate

Action To check the SFM LED status, remove the component cover and look on the SFM faceplate at the back of the M40e and M160 routers (see Figure 144 on page 348). Table 85 describes the SFM LED states.

Table 85: SFM LEDs

Color	Label	State	Description
Green	OK	On steadily	SFM is functioning normally.
		Blinking	SFM is starting up.
Amber	FAIL	On steadily	SFM has failed.

Step 4: Display the SFM Environmental Status

Action To display the SFM environmental information, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                   Status     Measurement
Power PEM 0                  OK
      PEM 1                  OK
Temp
[...Output truncated...]
      SPP 0                  OK         37 degrees C / 98 degrees F
      SPR 0                  OK         46 degrees C / 114 degrees F
      SPP 1                  OK         38 degrees C / 100 degrees F
      SPR 1                  OK         48 degrees C / 118 degrees F
      SPP 2                  OK         39 degrees C / 102 degrees F
      SPR 2                  OK         54 degrees C / 129 degrees F
      SFM 3                  Offline
[...Output truncated...]
```

What it Means The command output displays the status and temperature for the SFM and its two serialized components: the SPP card and the SPR card.

Alternative Action If there is a problem with the SFM status, you can display more detailed environmental information with the following CLI command:

user@host> **show chassis environment sfm**

```
user@host> show chassis environment sfm
SFM 0 status:
  State                           Online
  SPP temperature              36 degrees C / 96 degrees F
  SPR temperature              45 degrees C / 113 degrees F
  SPP Power:
    1.5 V                    1501 mV
    2.5 V                    2485 mV
    3.3 V                    3291 mV
    5.0 V                    5020 mV
    5.0 V bias               4974 mV
  SPR Power:
    1.5 V                    1501 mV
    2.5 V                    2492 mV
    3.3 V                    3301 mV
    5.0 V                    5028 mV
    5.0 V bias               4986 mV
    8.0 V bias               8305 mV
  CMB Revision                 12
SFM 1 status:
  [...Output truncated...]
SFM 2 status:
  [...Output truncated...]
SFM 3 status:
  State                           Offline
 - Hard FPC error
  [...Output truncated...]
```

The command output displays the SFM slot, status, and temperature of the air flowing past the SPP card and the SPR card. It also displays information about the SFM power supplies. The chassis management bus (CMB) slave revision level is also displayed.

You can display the environmental status of a particular SFM with the following CLI command:

user@host> **show chassis environment sfm** *sfm-lot*

Displaying SFM Alarms

Steps To Take To display SFM alarms and error messages, follow these steps:

1. Display Current SFM Alarms on page 353

2. Display SFM Error Messages in the System Log File on page 353

3. Display SFM Error Messages in the Chassis Daemon Log File on page 354

Step 1: Display Current SFM Alarms

Action To display the current SFM alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
4 alarms currently active
Alarm time               Class  Description
2002-05-14 09:23:58 PDT  Major  SFM Failure
2002-05-14 09:23:55 PDT  Major  SFM Failure
2002-05-14 09:23:53 PDT  Major  SFM Failure
2002-05-14 09:20:51 PDT  Major  No SFM Online, the box is not forwarding
```

What it Means The command output displays the alarm date, time, severity level, and description.

Step 2: Display SFM Error Messages in the System Log File

Action To display the SFM error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jun 11 20:31:11 hissy-re0 craftd[556]:  Major alarm set, No SFM Online, the box
is not forwarding
Jun 11 20:31:11 hissy-re0 alarmd[555]: Alarm set: SFM color=RED, class=CHASSIS,
reason=No SFM Online,
the box is not forwarding
```

What it Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match sfm command to see error messages that are generated when an SFM fails or is offline. Use this information to diagnose a power supply problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference.*

Step 3: Display SFM Error Messages in the Chassis Daemon Log File

The chassis daemon (chassisd) log file keeps track of the state of each chassis component.

Action To display the SFM error messages logged in the chassis daemon, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x0
Jun 11 20:50:16 bp_handle_button_intr button status 0x0
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x8
Jun 11 20:50:16 bp_handle_button_intr button status 0x8
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x8
Jun 11 20:50:16 bp_handle_button_intr button status 0x8
Jun 11 20:50:16 received second FPM key press, clearing timer!
Jun 11 20:50:18 bp_button_timer: taking sfm 1 offline
Jun 11 20:50:18 take_sfm_offline - slot 1 reason 7
Jun 11 20:50:18 cleaning up sfm 1 connection
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Blue LED Off [0x16]
Jun 11 20:50:18 SPP 1 - Blue LED Off
Jun 11 20:50:18 send: fpc 0, sfm 1 offline
Jun 11 20:50:18 send: fpc 1, sfm 1 offline
Jun 11 20:50:18 send: fpc 2, sfm 1 offline
Jun 11 20:50:18 send: fpc 6, sfm 1 offline
Jun 11 20:50:18 send: fpc 7, sfm 1 offline
Jun 11 20:50:18 fpc 2, sfm 1 offline ack
Jun 11 20:50:18 fpc 2, sfm 1 offline ack, online 0xc7 online-acks 0x4
Jun 11 20:50:18 fpc 1, sfm 1 offline ack
Jun 11 20:50:18 fpc 1, sfm 1 offline ack, online 0xc7 online-acks 0x6
Jun 11 20:50:18 fpc 0, sfm 1 offline ack
Jun 11 20:50:18 fpc 0, sfm 1 offline ack, online 0xc7 online-acks 0x7
Jun 11 20:50:18 fpc 7, sfm 1 offline ack
Jun 11 20:50:18 fpc 7, sfm 1 offline ack, online 0xc7 online-acks 0x87
Jun 11 20:50:18 fpc 6, sfm 1 offline ack
Jun 11 20:50:18 fpc 6, sfm 1 offline ack, online 0xc7 online-acks 0xc7
Jun 11 20:50:18 sfm_offline_now plane 1 conn 0x8152638
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert PLL Bypass [0x13]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert Board Reset [0x2e]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert ASIC Reset [0x28]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Disable Power [0x10]
Jun 11 20:50:18 SPP 1 - Disable Power [addr 0x9 cmd 0x10]
Jun 11 20:50:18 CMB readback SPP 1 [0xe9, 0xf2] -> 0x26
Jun 11 20:50:18 power disable verified, SPP 1
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Blue LED Off [0x16]
Jun 11 20:50:18 SPP 1 - Blue LED Off
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Green LED Off [0x1a]
Jun 11 20:50:18 SPP 1 - Green LED Off
Jun 11 20:50:18 check_sfm_online_alarm: present 0xf waiting 0x0 online 0xd
Jun 11 20:50:18 send_pfe_status(): sfm 0, sfm_online_mask 0xd fpc_online_mask
0xc7
Jun 11 20:50:18 send_pfe_status(): sfm 2, sfm_online_mask 0xd fpc_online_mask
0xc7
[...Output truncated...]
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the chassisd log file by using the | match “item |item |item” command. For example, | match “sfm|kernel|tnp”is a search for error messages for the SFM, kernel, and Trivial Networking Protocol (TNP), and indicates communication issues between the Routing Engine and the Packet Forwarding Engine components.

Verifying SFM Failure

Steps To Take To verify SFM failure, follow these steps:

1. Check the SFM Connection on page 355
2. Check the SFM Fuses on page 355
3. Perform an SFM Swap Test on page 356

Step 1: Check the SFM Connection

Action To check the SFM connection, make sure that it is properly seated in the midplane. Check the thumbscrews on the ejector locking tabs.

Step 2: Check the SFM Fuses

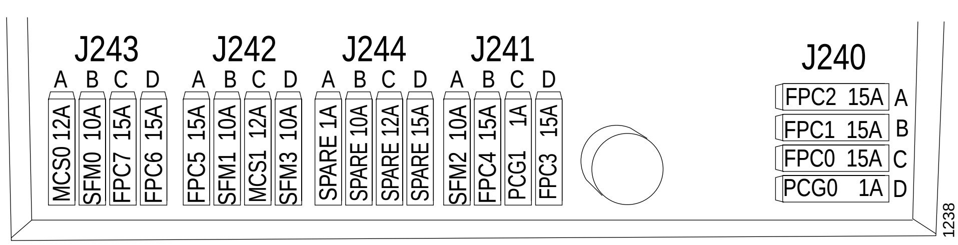
Action Check for blown SFM fuses.

The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly. You must remove the lower impeller assembly to access the fuses, as described in the *M40e Router Hardware Guide*.

When the fuse for an SFM blows, the SFM stops functioning even though it is installed correctly and the power supplies are providing power to the router.

For the M40e and M160 routers, when a fuse has blown but the power supplies are still delivering power to router, the amber LED adjacent to the fuse lights. See Figure 146.

Figure 146: M40e M160 Router Fuses



Another indication that a fuse has blown is that the colored indicator bulb inside it becomes visible through the clear cover on the fuse. For information about the indicator bulb color for each fuse type, see the appropriate router hardware guide.

A blown fuse can cause a component to fail even though it is correctly installed and the power supplies are functioning. Check for a blown fuse in the following circumstances:

- The LED that indicates normal operation for the component fails to light.
- The appropriate CLI show chassis environment command indicates that the component is installed but is not receiving power.

Step 3: Perform an SFM Swap Test

NOTE: Before performing a swap test, always check for bent pins in the midplane and check the SFM for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an SFM, follow these steps:

1. Remove the chassis rear component cover by loosening the screws on the corners of the cover and pulling it straight out from the chassis.
2. Remove the SFM, as described in the M40e and M160 router hardware guides.
3. Take the SFM offline by doing one of the following:
   - Use the following CLI command:

     user@host> **request chassis sfm slot** *slot-number* **offline**

   - Press and hold the offline button on the SFM faceplate at the rear of the router until the SFM OK LED turns off (about 5 seconds).
4. Replace the SFM with one that you know works.
5. Bring the SFM online by doing one of the following:
   - Use the following CLI command:

     user@host> **request chassis sfm slot** *slot-number* **online**

   - Press and hold the offline button on the SFM faceplate until the green OK LED lights (about 5 seconds).
6. Reinstall the rear component cover and tighten the screws to secure it to the chassis.
7. Check the SFM status. See “Display the SFM Summary Status” on page 349.

Getting SFM Hardware Information

Steps To Take To get the hardware information you need to return a failed SFM, follow these steps:

1. Display SFM Hardware Information on page 357
2. Locate the SFM Serial Number ID Label on page 357

Step 1: Display SFM Hardware Information

Action To display the SFM hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

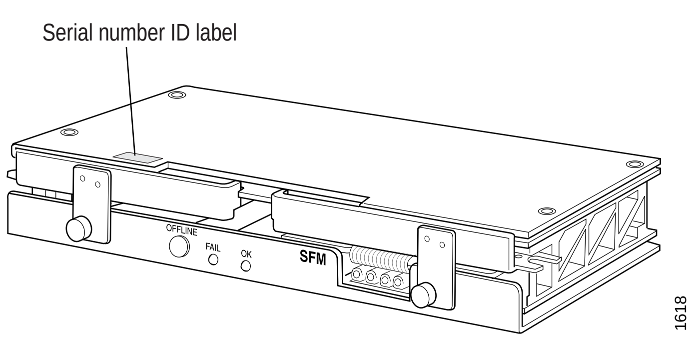
```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                20079             M160
[...Output truncated...]
SFM 0 SPP        REV 04   710-001228   AA2860
SFM 0 SPR        REV 01   710-001224   AB0139            Internet Processor I
SFM 1 SPP        REV 04   710-001228   AA2859
SFM 1 SPR        REV 02   710-001224   AA9861            Internet Processor I
SFM 2 SPP        REV 06   710-001228   AB3082
SFM 2 SPR
SFM 3 SPP        REV 04   710-001228   AA1998
SFM 3 SPR        REV 01   710-001224   AB0137            Internet Processor I
[...Output truncated...]
```

What it Means The command output displays the SFM slot number and SFM serial component (SPP and SPR) card names, SFM revision level, part number, serial number, and description.

Step 2: Locate the SFM Serial Number ID Label

Action To locate the SFM serial number ID label, look on the left side of the SFM top panel (see Figure 147).

Figure 147: SFM Serial Number ID Label



Replacing the SFM

The SFMs are hot-removable and hot-insertable. You can remove and replace SFMs without powering down the router or disrupting the routing functions. However, you must take an SFM offline before replacing it.

Inserting or removing an SFM causes a brief interruption in forwarding performance (about 500 ms) as the Packet Forwarding Engine reconfigures the distribution of packets across the remaining SFMs.

Action To replace an SFM, see "Return the Failed Component" on page 86, or the procedure to return a field-replaceable unit in the M40e or M160 router hardware guide.

Chapter 27
Monitoring the MCS

You monitor and maintain the Miscellaneous Control Subsystem (MCS) to provide control and monitoring functions for router components and to provide SONET/SDH clocking for the M40e and M160 routers. (See Table 86.)

Table 86: Checklist for Monitoring the MCS

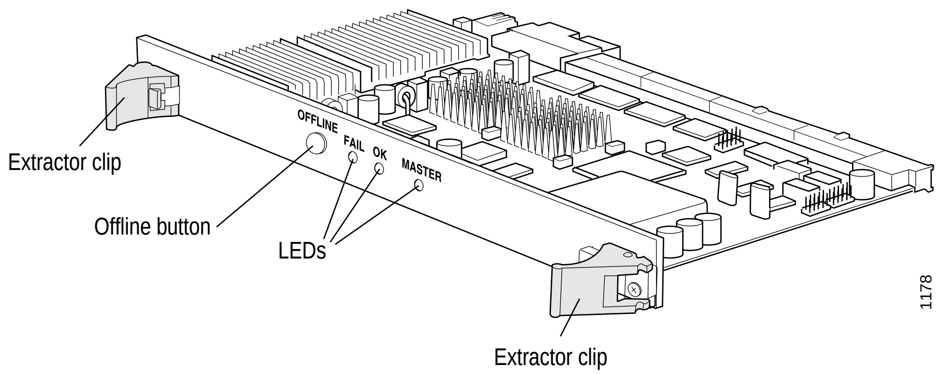
Monitor MCS Tasks	Command or Action
Understanding the MCS on page 360	
Checking the MCS Status on page 362	
1. Check the MCS Environmental Status on page 362	show chassis environment mcs
2. Check the MCS Status from the Craft Interface on page 363	show chassis craft-interface
3. Check the MCS LEDs on page 364	Check the LEDs on the MCS faceplate.
Verifying MCS Failure on page 365	
1. Check the MCS Fuses on page 365	The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly.
2. Perform an MCS Swap Test on page 366	Remove the MCS and replace it with one that you know works.
Getting MCS Hardware Information on page 367	
1. Display the MCS Hardware Information on page 367	show chassis hardware
2. Locate the MCS Serial Number ID Label on page 368	Look at the bottom left of the MCS board.
Returning the MCS on page 368	See "Return the Failed Component" on page 86, or follow the procedure in the M40e or M160 router hardware guide.

Understanding the MCS

Purpose Inspect the MCS to ensure that control and monitoring functions for router components and SONET/SDH clocking for the router function normally.

What Is an MCS The MCS is a component of the host module on M40e and M160 routers (see Figure 148). The MCS works with the Routing Engine to provide control and monitoring functions for router components and to provide SONET/SDH clocking for the router.

Figure 148: MCS Component



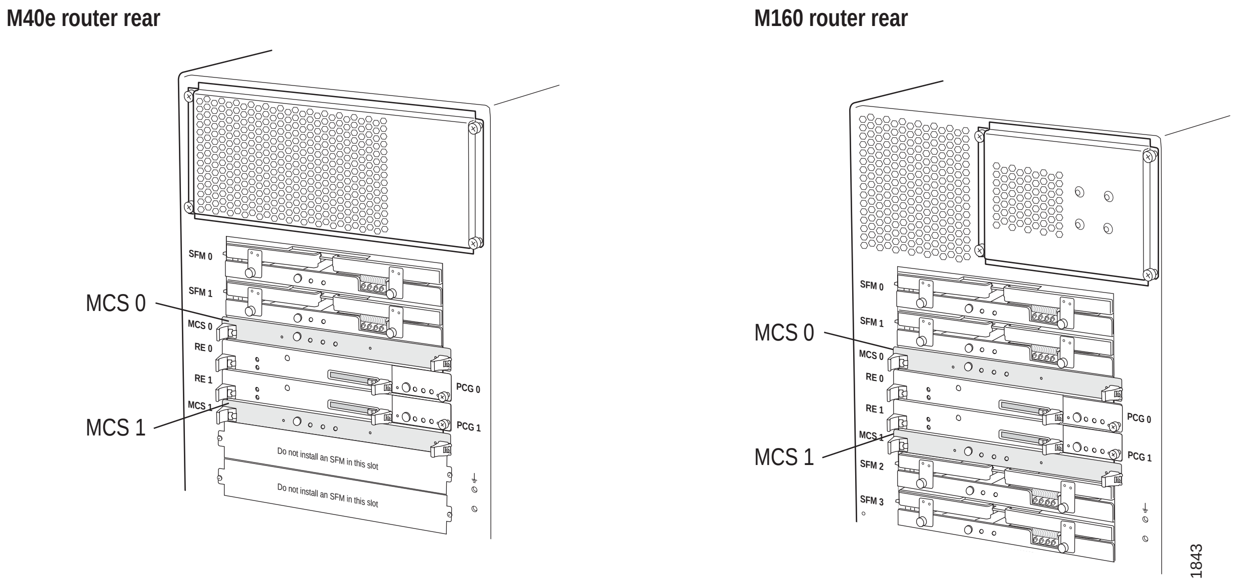
The router can be equipped with up to two MCSs for redundancy. If two MCSs are installed, one acts as the master MCS and the other acts as a backup. If the master MCS fails or is removed, the backup MCS restarts and becomes the master MCS.

NOTE: The host modules (RE0 working with MCS0 and RE1 working with MCS1) actually have the master and backup role.

Each MCS requires a Routing Engine to be installed in an adjacent slot. MCS0 installs above RE0, and MCS1 installs below RE1. Even if an MCS is physically installed in the chassis, it does not function if there is no Routing Engine present in the adjacent slot.

The MCS installs into the midplane from the back of the chassis (see Figure 149).

Figure 149: M40e and M160 Router MCS Location



See Also

- Monitoring the Host Module on page 341
- Monitoring the Routing Engine on page 125
- Monitoring Redundant Routing Engines on page 491
- Monitoring Redundant MCSs on page 567

Checking the MCS Status

Steps To Take To check the MCS status, follow these steps:

1. Check the MCS Environmental Status on page 362
2. Check the MCS Status from the Craft Interface on page 363
3. Check the MCS LEDs on page 364

Step 1: Check the MCS Environmental Status

Action To check the MCS environmental status, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis environment mcs**

Sample Output

```
user@host> show chassis environment mcs
MCS 0 status:
  State                           Online Master
  Temperature                  43 degrees C / 109 degrees F
  Power:
    3.3 V                    3318 mV
    5.0 V                    4974 mV
    12.0 V on                  12
  FPGA Revision                13
MCS 1 status:
  State                           Online Standby
  Temperature                  58 degrees C / 136 degrees F
  Power:
    3.3 V                    3317 mV
    5.0 V                    5006 mV
    12.0 V                  11843 mV
    5.0 V bias               4998 mV
    8.0 V bias               8195 mV
  BUS Revision                 12
  FPGA Revision               255
```

What It Means The show chassis environment mcs command is available on the M40e and M160 routers only. The command output displays environmental information about both MCSs installed in the router or about an individual MCS. The MCS status can be Present, Online, Offline, or Empty. The command also indicates that the MCS is the master MCS. The command output also displays the temperature of the air flowing past the MCS, information about MCS power supplies, field-programmable gate array (FPGA) revision information, and the revision level of the chassis management bus (CMB) slave.

Alternative Action To display the environmental status of a particular MCS, use the following JUNOS CLI operational mode command:

user@host> **show chassis environment mcs** *slot*

Step 2: Check the MCS Status from the Craft Interface

Action To display the MCS LED status from the craft interface, use the following JUNOS software operational mode CLI command:

user@host> **show chassis craft-interface**

Sample Output

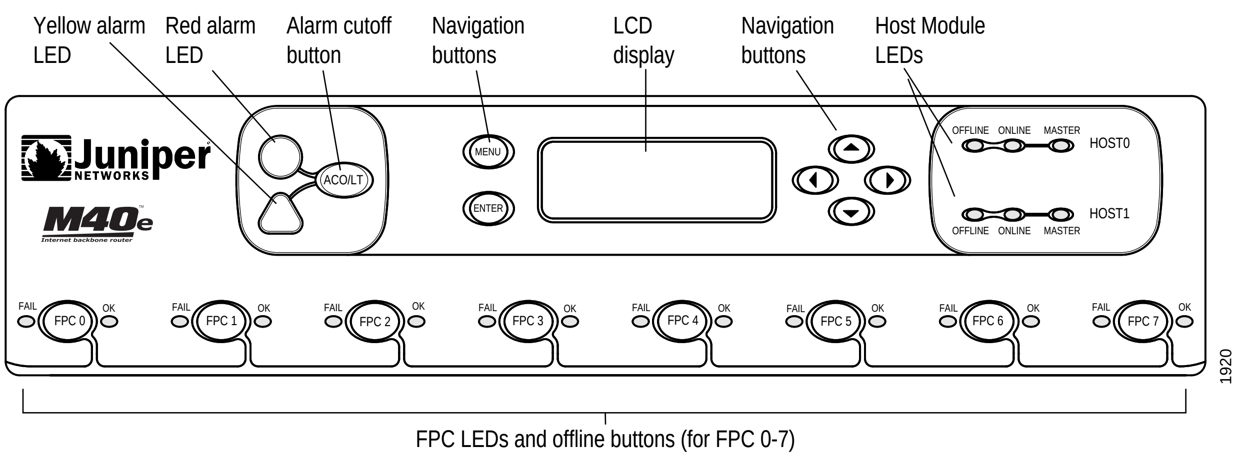
```
user@host> show chassis craft-interface
[...Output truncated...]

    MCS and SFM LEDs:
    MCS    0   1      SFM    0   1   2   3
    --------------------------------------
    Amber      .             .   .
    Green      .             .   .
    Blue       *             *   *
```

What It Means If the amber FAIL LED is on, check for current MCS alarms.

Alternative Action Look at the Host Module LEDs on the craft interface. The LEDs indicate the MCS status. (See Figure 150.)

Figure 150: M40e and M160 Router Craft Interface Host Module LEDs



Three host module LEDs—one green MASTER, one green ONLINE, and one red OFFLINE—located on the upper right of the craft interface indicate the status of each host module. The LEDs marked HOST0 show the status of the Routing Engine in slot RE0 and the MCS in slot MCS0. The LEDs marked HOST1 show the status of the Routing Engine in slot RE1 and the MCS in slot MCS1.

Table 87 describes the functions of the host module LEDs.

Table 87: Host Module LEDs

Label	Shape	Color	State	Description
MASTER	○	Green	On steadily	Host module (Routing Engine and MCS) is functioning as master.
ONLINE	○	Green	On steadily	Host module is present and operational.
			Blinking	Host module is starting up.
OFFLINE	○	Red	On steadily	Host module is not present, or is present but not operational.

Step 3: Check the MCS LEDs

Action To check the MCS status, look at the LEDs on the MCS faceplate.

Table 88 describes the functions of these LEDs.

Table 88: MCS LEDs

Color	Label	State	Description
Blue	MASTER	On steadily	MCS is master.
Green	OK	On steadily	MCS is operating normally.
		Blinking	MCS is starting up.
Amber	FAIL	On steadily	MCS has failed.

When the MCS is functioning normally, the green OK LED remains on steadily. If the amber FAIL LED is on, check for MCS alarms.

Verifying MCS Failure

Steps To Take To verify MCS operation failure, follow these steps:

1. Check the MCS Fuses on page 365
2. Perform an MCS Swap Test on page 366

Step 1: Check the MCS Fuses

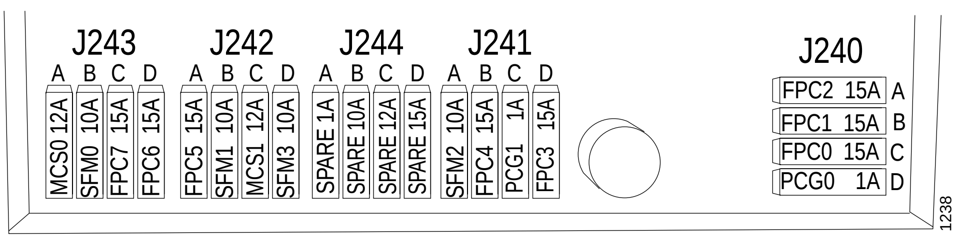
Action Check the MCS fuses to check for failure.

The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly. You must remove the lower impeller assembly to access the fuses, as described in the appropriate router hardware guide.

When the fuse for an MCS blows, the MCS stops functioning even though it is installed correctly and the power supplies are providing power to the router.

For the M40e and M160 routers, when a fuse has blown but the power supplies are still delivering power to router, the amber LED adjacent to the fuse lights. See Figure 151.

Figure 151: M40e M160 Router Fuses



Another indication that a fuse has blown is that the colored indicator bulb inside it becomes visible through the clear cover on the fuse. For information about the indicator bulb color for each fuse type, see the appropriate router hardware guide.

A blown fuse can cause a component to fail even though it is correctly installed and the power supplies are functioning. Check for a blown fuse in the following circumstances:

- The LED that indicates normal operation for the component fails to light.
- The appropriate CLI show chassis environment command indicates that the component is installed but is not receiving power.

Step 2: Perform an MCS Swap Test

The MCS can fail and not start, or it can cause a connectivity problem between the Routing Engine and the Packet Forwarding Engine components, such as the Flexible PIC Concentrator (FPC) and Switching and Forwarding Module (SFM). You can perform a swap test on the MCS to try to pinpoint the problem.

CAUTION: The MCS is hot-pluggable. Routing functions are interrupted until a replacement is installed. You should perform a swap test during a maintenance window.

Before performing a swap test, always check for bent pins in the midplane and check the MCS for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an MCS, remove it and replace it with one that you know works.

Normally, if two host modules are installed in the router, HOST0 functions as the master and HOST1 as the backup. You can remove the backup host module (or either of its components) without interrupting the functioning of the router. If you take the master host module offline, the router reboots and the backup host module becomes the master. If the router has only one host module, taking it offline causes the router to shut down.

The host module is taken offline and brought back online as a unit. Before you replace the Routing Engine or an MCS, you must take the host module offline; the host module is hot-pluggable.

To remove an MCS, follow these steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the Routing Engine.

2. Attach an electrostatic discharge (ESD) strap to your bare wrist and connect the strap to one of the ESD points on the chassis.

3. Remove the rear component cover by loosening the screws at the corners of the cover and pulling it straight off of the chassis.

4. If two host modules are installed, check whether the MCS you are removing belongs to the master host module. Use the show chassis environment mcs CLI command or check the MCS LEDs. If it does, switch mastership to the standby host module. You can change the default mastership by including the routing-engine statement at the [edit chassis redundancy] hierarchy level in the configuration, as described in the *JUNOS System Basics Configuration Guide*.

5. On the console or other management device connected to the Routing Engine that is paired with the MCS you are removing, enter CLI operational mode and issue the following command. The command shuts down the Routing Engine cleanly, so its state information is preserved.

   user@host> **request system halt**

   Wait to continue until all software processes have shut down.

6. Flip the ends of the extractor clips outward.

7. Grasp the extractor clips and slide the unit about halfway out of the chassis.

8. Place one hand under the MCS to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

9. Align the rear of the MCS with the guides inside the chassis and slide it in completely.

10. Press the extractor clips on the left and right sides of the MCS inward.

11. Verify that the green LED labeled OK on the MCS faceplate is lit. Also check the host module LEDs on the craft interface to verify that the green LED labeled ONLINE is lit for the host module to which the MCS belongs.

    You can also verify correct MCS functioning by using the show chassis environment mcs command.

12. Reinstall the rear component cover and tighten the screws at the corners to secure it to the chassis.

Getting MCS Hardware Information

Steps To Take To get MCS hardware information, follow these steps:

1. Display the MCS Hardware Information on page 367
2. Locate the MCS Serial Number ID Label on page 368

Step 1: Display the MCS Hardware Information

Action To display the MCS hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

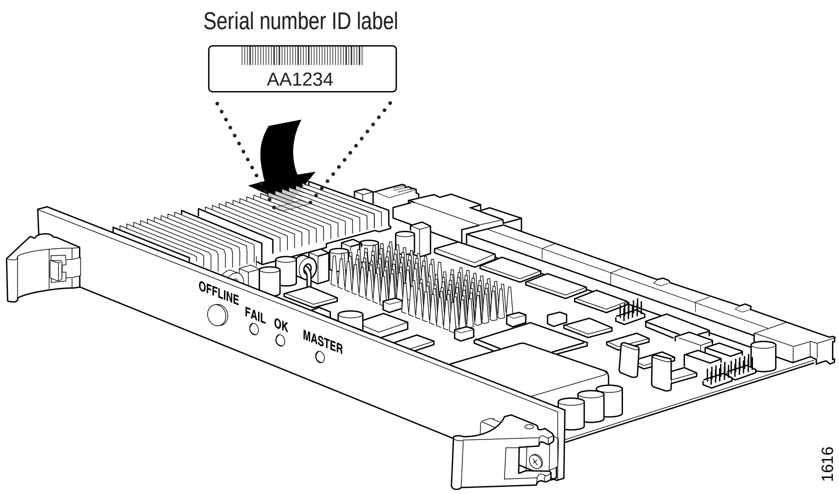
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                                  M40e
[...Output truncated...]
Routing Engine 0                       d8000007c8460a01  RE-2.0
MCS 0            REV 11   710-001226   AS4709
[...Output truncated...]
```

What It Means The command output displays the MCS slot number, revision level, part number, and serial number. Give this information to the Juniper Networks Technical Assistance Center (JTAC) if the MCS fails.

Step 2: Locate the MCS Serial Number ID Label

Action To locate the MCS serial number ID label, look on the bottom left side of the board, as shown in Figure 152.

Figure 152: MCS Serial Number ID Label



Returning the MCS

Action To return the MCS, see “Replacing a Failed Component” on page 122, or the procedure to return a field-replaceable unit in the M40e or M160 router hardware guide.

Chapter 28

Monitoring the PCG

You monitor the Packet Forwarding Engine Clock Generator (PCG) to ensure that a clocking signal is generated to synchronize the internal M40e and M160 router Packet Forwarding Engine components. (See Table 89.)

Table 89: Checklist for Monitoring the PCG

Monitor PCG Tasks	Command or Action
Understanding the PCG on page 370	
Monitoring the PCG Status on page 371	
1. Monitor the PCG Environmental Status on page 371	show chassis environment show chassis environment pcg
2. Display the PCG LED States at the Command Line on page 372	show chassis craft-interface
3. Look at the PCG LEDs on the Faceplate on page 373	Remove the rear component cover and look on the PCG faceplate at the back of the M40e or M140 router chassis.
Determining PCG Mastership on page 373	
1. Display the PCG Master in the Craft Interface Output on page 373	show chassis craft-interface
2. Look at the PCG LEDs on the Faceplate on page 374	Remove the rear component cover and look on the PCG faceplate at the rear of the M40e or M160 router chassis.
3. Display the Packet Forwarding Engine Current Clock Source on page 374	show chassis clocks
Displaying PCG Alarms on page 375	
1. Display Current PCG Alarms on page 375	show chassis alarms
2. Display PCG Error Messages in the System Log File on page 375	show log messages
3. Display PCG Error Messages in the Chassis Daemon Log File on page 375	show log chassisd
Verifying PCG Failure on page 376	
1. Check the PCG Connection on page 376	Check the thumbscrew on the right side of the PCG.
2. Check the PCG Fuses on page 377	The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly.

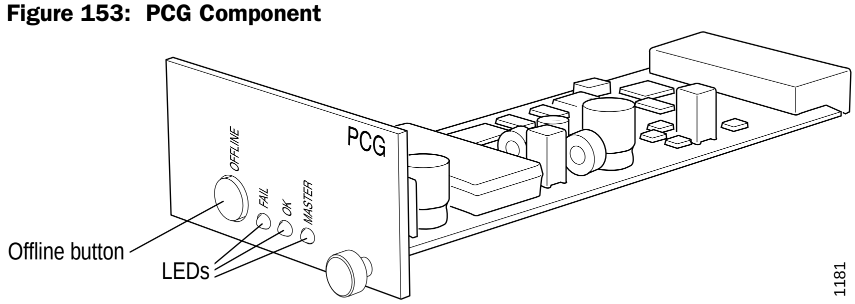
Monitor PCG Tasks	Command or Action
3. Perform a PCG Swap Test on page 378	1. Take the PCG offline. 2. Replace the PCG with one that you know works. 3. Bring the PCG online. 4. Check the PCG status.
Getting PCG Hardware Information on page 378	
1. Display the PCG Hardware Information on page 379	show chassis hardware
2. Locate the PCG Serial Number ID Label on page 379	Look on the top of the PCG, close to the midplane connector.
Replacing the PCG on page 379	See "Return the Failed Component" on page 86, or follow the procedure in the M40e or M160 router hardware guide.

Understanding the PCG

Purpose You monitor the PCGs to ensure that they generate a clock signal to synchronize the modules and application-specific integrated circuits (ASICs) that make up the Packet Forwarding Engine.

What Is a PCG The PCG supplies a 125-MHz system clock to synchronize the modules and ASICs that make up the Packet Forwarding Engine (see Figure 153).

Figure 153: PCG Component



A router has two PCGs. They are located at the rear of the chassis in the slots labeled PCG0 and PCG1, to the right of the Routing Engine slots.

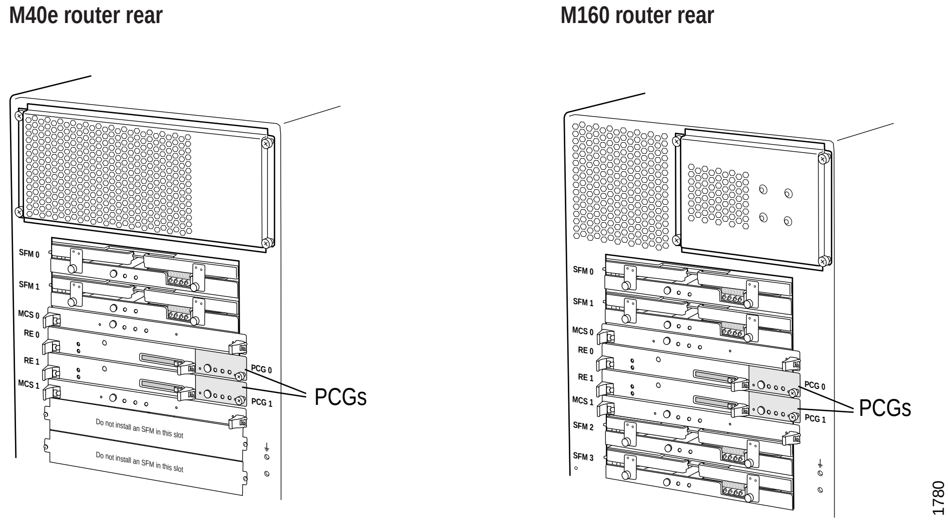
Both PCGs send clock signals to the Packet Forwarding Engine modules, along with a signal indicating which is the master clock source. The master Routing Engine controls which PCG is master and which is backup.

The PCGs are field-replaceable and hot-pluggable. You can remove and replace them without powering down the router; however, the routing functions of the system are interrupted when a PCG is removed.

Removing the backup PCG does not affect the functioning of the router. Taking the master PCG offline causes the Flexible PIC Concentrators (FPCs) and Switching and Forwarding Modules (SFMs) to power down and restart with the other PCG selected as master. The forwarding and routing functions are interrupted during this process.

Figure 154 shows the location of the PCGs on the M40e and M160 router chassis.

Figure 154: M40e and M160 Router PCG Location



Monitoring the PCG Status

Steps To Take To monitor the PCG status, follow these steps:

1. Monitor the PCG Environmental Status on page 371
2. Display the PCG LED States at the Command Line on page 372
3. Look at the PCG LEDs on the Faceplate on page 373

Step 1: Monitor the PCG Environmental Status

Action To monitor the PCG environment status, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                  Status     Measurement
Power PEM 0                 OK
      PEM 1                 OK
Temp  PCG 0                 OK         41 degrees C / 105 degrees F
      PCG 1                 OK         39 degrees C / 102 degrees F
[...Output truncated...]
```

What It Means The command output displays the status and temperature for each PCG.

Alternative Action If there is a problem with the PCG status, you can display more detailed PCG environmental information with the following CLI command:

user@host> **show chassis environment pcg**

The command output is as follows:

```
user@host> show chassis environment pcg
PCG 0 status:
  State                            Online - PFE clock source
  Temperature                   41 degrees C / 105 degrees F
  Frequency:
    Setting                 125.00 MHz
    Measurement             125.03 MHz
  Power:
    3.3 V                     3266 mV
    5.0 V bias                4981 mV
    8.0 V bias                8168 mV
  CMB Revision                  12
PCG 1 status:
  State                            Online
  Temperature                   39 degrees C / 102 degrees F
  Frequency:
    Setting                 125.00 MHz
    Measurement             125.03 MHz
  Power:
    3.3 V                     3271 mV
    5.0 V bias                4971 mV
    8.0 V bias                8175 mV
  CMB Revision                  12
```

The command output displays the status for each PCG slot 0 and 1. The operating status can be Present, Online, Offline, or Empty. If Online, it can be the current PFE clock source or backup. The command output displays the temperature of the air flowing past the PCG and the frequency setting and measurement for the PCG. The command output also displays information about the PCG power supplies and the revision level of the chassis management bus (CMB) slave.

Step 2: Display the PCG LED States at the Command Line

Action To display the PCG LED states, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
PCG LEDs:
  PCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

[...Output truncated...]
```

What It Means The command output is for an M160 router. The PCGs in slots 0 and 1 are online and are functioning normally. The status colors represent the possible PCG operating states: Amber (Fail), Green (OK), and Blue (Master). The (*) indicates the current operating state.

Step 3: Look at the PCG LEDs on the Faceplate

Action To view the PCG LEDs, remove the rear component cover and look on the PCG faceplate at the rear of the M40e or M160 router chassis (see Figure 153 on page 370 and Figure 154 on page 371). Table 90 describes the functions of these LEDs.

Table 90: PCG LEDs

Color	Label	State	Description
Blue	MASTER	On steadily	PCG is master.
Green	OK	On steadily	PCG is operating normally.
		Blinking	PCG is starting up.
Amber	FAIL	On steadily	PCG has failed.

Determining PCG Mastership

The PCGs function as redundant components. For information about monitoring redundant PCGs, see "Monitoring Redundant PCGs" on page 595.

Steps To Take To determine which PCG is operating as the master, follow these steps:

1. Display the PCG Master in the Craft Interface Output on page 373
2. Look at the PCG LEDs on the Faceplate on page 374
3. Display the Packet Forwarding Engine Current Clock Source on page 374

Step 1: Display the PCG Master in the Craft Interface Output

Action To determine the PCG master from the craft interface status information, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
PCG LEDs:
  PCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

[...Output truncated...]
```

What It Means The command output shows that PCG 0 is the master because the blue MASTER LED is on.

Step 2: Look at the PCG LEDs on the Faceplate

Action To check the PCG LEDs, look on the PCG faceplate at the rear of the M40e or M160 router chassis (see Figure 153 on page 370 and Figure 154 on page 371). Table 90 describes the PCG LED states. If the blue MASTER LED on the PCG faceplate is on steadily, the PCG is functioning as master.

Step 3: Display the Packet Forwarding Engine Current Clock Source

The Packet Forwarding Engine current clock source is the master PCG.

Action To display the PCG master from the Packet Forwarding Engine clock source output, use the following CLI command:

user@host> **show chassis clocks**

Sample Output

```
user@host> show chassis clocks
PFE clock status:
  Current source           PCG 0
  Measured frequency       125.03 MHz
Reference clock status:
  Current source           Primary
  Primary source           Internal
  Secondary source         Internal
  Tertiary source          Internal
  Rollover algorithm       Holdover
  PLL mode                 Free-running
  PLL errors               0
  Sync message current     0x00
  Sync message normal      0x00
  Sync message override    0x00
```

What It Means The command output shows that the PCG in slot 0 is the primary clock source.

Displaying PCG Alarms

Steps To Take To display PCG alarms and error messages, follow these steps:

1. Display Current PCG Alarms on page 375
2. Display PCG Error Messages in the System Log File on page 375
3. Display PCG Error Messages in the Chassis Daemon Log File on page 375

Step 1: Display Current PCG Alarms

Action To display the current PCG alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
2 alarms currently active
Alarm time              Class  Description
2002-06-11 20:30:29 PDT  Minor PCG 0 Not Online
2002-06-11 20:30:32 PDT  Minor No PCGs Online
```

What It Means The command output displays the alarm date, time, severity level, and description.

Step 2: Display PCG Error Messages in the System Log File

Action To display the PCG error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jun 11 20:31:31 myrouter chassisd[553]: CHASSISD_NO_GOOD_PCGS:
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match pcgs command to see error messages that are generated when a PCG fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display PCG Error Messages in the Chassis Daemon Log File

Action To display the PCG error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jun 11 20:31:17 FPC 7 - Disable Power [addr 0x17 cmd 0x10]
Jun 11 20:31:17 CMB readback FPC 7 [0xf7, 0xf2] -> 0x26
Jun 11 20:31:17 power disable verified, FPC 7
Jun 11 20:31:17 CHASSISD_IFDEV_DETACH: ifdev_detach(7)
Jun 11 20:31:17 ifd so-7/0/0 marked as gone
Jun 11 20:31:19 PCG 0 set alarm 0x3
Jun 11 20:31:19 alarm op fru 1 op 1 reason 3
Jun 11 20:31:19 send: yellow alarm set, class 100 obj 110 reason 3
Jun 11 20:31:19 CMB cmd to PCG 0 [0xe2], Disable Power [0x10]
Jun 11 20:31:19 PCG 0 - Disable Power [addr 0x2 cmd 0x10]
Jun 11 20:31:19 CMB readback PCG 0 [0xe2, 0xf2] -> 0x6
Jun 11 20:31:19 power disable verified, PCG 0
Jun 11 20:31:19 CMB cmd to PCG 0 [0xe2], Blue LED Off [0x16]
Jun 11 20:31:19 PCG 0 - Blue LED Off
Jun 11 20:31:19 CMB cmd to PCG 0 [0xe2], Green LED Off [0x1a]
Jun 11 20:31:19 PCG 0 - Green LED Off
Jun 11 20:31:19 CMB cmd to PCG 0 [0xe2], Amber LED Off [0x18]
Jun 11 20:31:19 PCG 0 - Amber LED Off
Jun 11 20:31:19 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:31:19 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x0
Jun 11 20:31:19 bp_handle_button_intr button status 0x0
Jun 11 20:31:21 reading FPC 0 initial state
Jun 11 20:31:21 CMB readback FPC 0 [0xf0, 0xff] -> 0xc
Jun 11 20:31:21 reading FPC 0 ideeprom
Jun 11 20:31:21 reading FPC 1 initial state
Jun 11 20:31:21 CMB readback FPC 1 [0xf1, 0xff] -> 0xc
Jun 11 20:31:21 reading FPC 1 ideeprom
Jun 11 20:31:21 reading FPC 2 initial state
Jun 11 20:31:21 CMB readback FPC 2 [0xf2, 0xff] -> 0xc
Jun 11 20:31:21 reading FPC 2 ideeprom
Jun 11 20:31:21 reading FPC 6 initial state
Jun 11 20:31:21 CMB readback FPC 6 [0xf6, 0xff] -> 0xc
Jun 11 20:31:21 reading FPC 6 ideeprom
Jun 11 20:31:21 reading FPC 7 initial state
Jun 11 20:31:21 CMB readback FPC 7 [0xf7, 0xff] -> 0xc
Jun 11 20:31:21 reading FPC 7 ideeprom
Jun 11 20:31:21 gen_sfm_wait_mask 0x0
Jun 11 20:31:21 ...power sequencer started...
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Verifying PCG Failure

Steps To Take To verify PCG failure, follow these steps:

1. Check the PCG Connection on page 376
2. Perform a PCG Swap Test on page 378

Step 1: Check the PCG Connection

Action To check the PCG connection, make sure the PCG is properly seated in the midplane. Check the thumbscrew on the right side of the PCG.

Step 2: Check the PCG Fuses

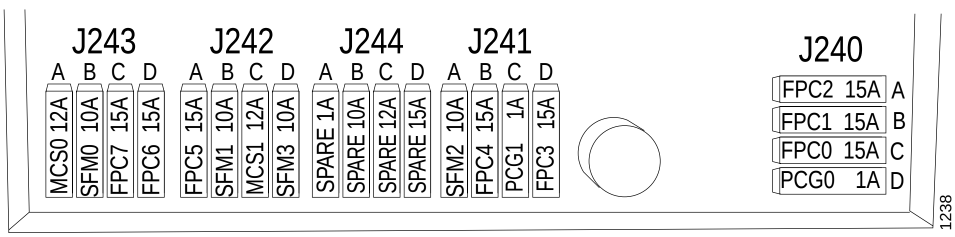
Action Check the PCG fuses to check for failure.

The M40e and M160 router fuses are located in a fuse box at the rear of the midplane, behind the lower rear impeller assembly. You must remove the lower impeller assembly to access the fuses, as described in the appropriate router hardware guide.

When the fuse for an PCG blows, the PCG stops functioning even though it is installed correctly and the power supplies are providing power to the router.

For the M40e and M160 routers, when a fuse has blown but the power supplies are still delivering power to router, the amber LED adjacent to the fuse lights. See Figure 155 on page 377.

Figure 155: M40e M160 Router Fuses



Another indication that a fuse has blown is that the colored indicator bulb inside it becomes visible through the clear cover on the fuse. For information about the indicator bulb color for each fuse type, see the appropriate router hardware guide.

A blown fuse can cause a component to fail even though it is correctly installed and the power supplies are functioning. Check for a blown fuse in the following circumstances:

- The LED that indicates normal operation for the component fails to light.
- The appropriate CLI show chassis environment command indicates that the component is installed but is not receiving power.

Step 3: Perform a PCG Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the PCG for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on a PCG, follow these steps:

1. Have an antistatic mat ready.
2. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
3. Remove the rear component cover by loosening the screws on the corners of the cover and pulling it straight out from the chassis.
4. Press the offline button on the faceplate of the PCG and hold it down until the Red FAIL LED lights (about 3 seconds).
5. Loosen the thumbscrew on the right side of the PCG.
6. Grasp the thumbscrew and slide out the PCG.
7. Align the rear of the PCG with the guides inside the chassis.
8. Slide the PCG all the way into the card cage until it contacts the midplane.
9. Tighten the thumbscrew on the right side of the PCG faceplate.
10. Verify that the PCG is properly installed by looking at the LEDs on the PCG faceplate. The green OK LED should light steadily.

Getting PCG Hardware Information

Steps To Take To get the PCG hardware information, follow these steps:

1. Display the PCG Hardware Information on page 379
2. Locate the PCG Serial Number ID Label on page 379

Step 1: Display the PCG Hardware Information

Action To display the PCG hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

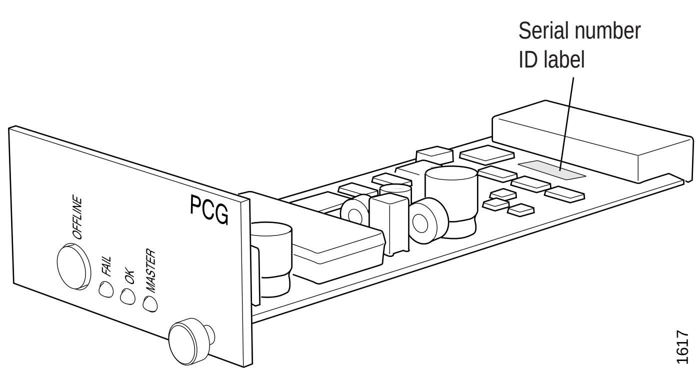
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                20079             M160
Midplane         REV 03   710-001245   AB4132
FPM CMB          REV 02   710-001642   AB3264
FPM Display      REV 02   710-001647   AB3046
CIP              REV 04   710-001593   AB3284
PEM 0            Rev 03   740-001243   KM28409           DC
PEM 1            Rev 03   740-001243   KM13359           DC
PCG 0            REV 02   710-001568   AB3013
PCG 1            REV 02   710-001568   AB3000
```

What It Means The command output displays the PCG slot number, revision level, part number, and serial number.

Step 2: Locate the PCG Serial Number ID Label

Action To locate the PCG serial number ID label, look on the top of the PCG, close to the midplane connector.

Figure 156: PCG Serial Number ID Label



Replacing the PCG

The PCGs are hot-pluggable. You can remove and replace them without powering down the router, but the routing functions of the system are interrupted when the PCG is removed.

If both PCGs are installed and functioning normally, PCG0 is the master PCG and PCG1 is the backup by default.

Removing the backup PCG does not affect the functioning of the router. Taking the master PCG offline causes the FPCs and SFMs to power down and restart, with the other PCG selected as master. The forwarding and routing functions are interrupted during this process.

Action To replace a PCG, see “Return the Failed Component” on page 86, or the procedure to return a field-replaceable unit in the M40e or M160 router hardware guide.

Chapter 29

Monitoring the CIP

You monitor the Connector Interface Panel (CIP) to ensure management connection to the M40e, M160, M320, T320, and T640 routing node Routing Engines, Building Integrated Timing Source (BITS) interfaces for the Miscellaneous Control Subsystem (MCS), and alarm relay contacts. (See Table 91.)

Table 91: Checklist for Monitoring the CIP

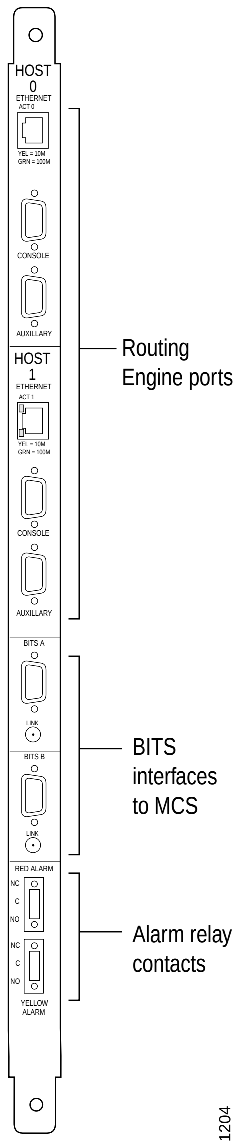
Tasks for Monitoring the CIP	Command or Action
Understanding the CIP on page 382	
Monitoring the CIP Status on page 384	show chassis environment
Checking for CIP Alarms on page 385	
1. Display Current CIP Alarms on page 385	show chassis alarms
2. Display CIP Error Messages in the System Log File on page 385	show log messages
3. Display CIP Error Messages in the Chassis Daemon Log File on page 386	show log chassisd
Verifying CIP Failure on page 386	
1. Check the CIP Connection on page 386	Check the connector screws on the CIP faceplate.
2. Check the Ethernet Port Functionality on page 386	1. Connect to the Ethernet port. 2. Check the LINK LED. 3. Run the JUNOS software CLI.
3. Performing a CIP Swap Test on page 387	1. Power down the router. 2. Remove the CIP. 3. Replace the CIP with one that you know works. 4. Power on the router.
Getting CIP Hardware Information on page 388	
1. Display CIP Hardware Information on page 388	show chassis hardware
2. Locating the CIP Serial Number ID Label on page 389	Look on the top of the left side of the CIP.
Replacing the CIP on page 389	Power down the router. To replace and return a CIP, follow the instructions in the M40e or M160 router hardware guide.

Understanding the CIP

Purpose Inspect the CIP to ensure connection to the Routing Engines, BITS interfaces for the MCS, and alarm relay contacts.

What Is the CIP The CIP provides an interface through which you can connect to the M40e and M160 Routing Engines, BITS interfaces for the MCS, and alarm relay contacts (see Figure 157).

Figure 157: CIP Component



The CIP has two sets of ports you use to connect the Routing Engines to external management devices. From these management devices, you can use the JUNOS software command-line interface (CLI) to configure and monitor the router.

The upper set of ports, labeled HOST0, connect to the Routing Engine in slot RE0, and the lower set of ports, labeled HOST1, connect to the Routing Engine in slot RE1.

Each HOST port set includes the following ports:

- ETHERNET—Connects the Routing Engine through an Ethernet connection to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management. The port uses an autosensing RJ-45 connector to support both 10-Mbps and 100-Mbps connections. Two small LEDs on the left edge of the port indicate the connection in use: the amber LED lights for a 10-Mbps connection and the green LED lights for a 100-Mbps connection.

- CONSOLE—Connects the Routing Engine to a system console through an RS-232 (EIA-232) serial cable.

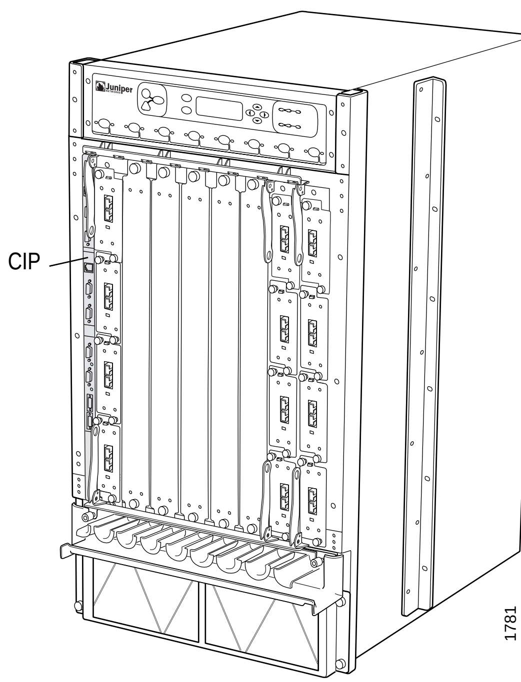
- AUXILIARY— Connects the Routing Engine to a laptop, modem, or other auxiliary device through an RS-232 (EIA-232) serial cable.

At the center of the CIP are two ports labeled BITS A and BITS B. These are the BITS connectors to the MCS. The router does not support BITS input, so these ports currently do not function.

The CIP has two sets of alarm relay contacts for connecting the router to external alarm devices. Whenever a system condition triggers either the red or yellow alarm on the craft interface, the alarm relay contacts are also activated. The alarm relay contacts are located below the BITS interface ports.

The CIP is located on the left side of the M40e and M160 router Flexible PIC Concentrator (FPC) card cage (see Figure 158).

Figure 158: M40e and M160 Router CIP Location



The CIP is field-replaceable, but is not hot-removable, hot-insertable, or hot-pluggable. You must power down the router before removing or installing it.

See Also

- Maintaining the Cable Management System, Cables, and Connectors on page 275
- Monitoring the Routing Engine on page 125

Monitoring the CIP Status

Action To monitor the CIP status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                 Status     Measurement
[...Output truncated...]
Misc  CIP                  OK
```

What It Means The command output displays the status for the CIP, which can be OK, Absent, or Failed.

Checking for CIP Alarms

Steps To Take To check for CIP alarms, follow these steps:

1. Display Current CIP Alarms on page 385
2. Display CIP Error Messages in the System Log File on page 385
3. Display CIP Error Messages in the Chassis Daemon Log File on page 386

Step 1: Display Current CIP Alarms

Action To display the current CIP alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
2 alarms currently active
Alarm time               Class  Description
2002-06-11 20:45:08 UTC  Major  Connector Interface Panel Missing
2002-06-11 20:45:07 UTC  Major  fxp0: ethernet link down
```

What It Means The command output displays the alarm date, time, severity level, and description. fxp0 is the Ethernet connection to a management LAN.

Step 2: Display CIP Error Messages in the System Log File

Action To display the CIP error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jun 11 20:45:07 hissy-re0 /kernel: fxp0: link media DOWN 10Mb / half-duplex
Jun 11 20:45:07 hissy-re0 craftd[556]:  Major alarm set, fxp0: ethernet link
down
Jun 11 20:45:07 hissy-re0 alarmd[555]: Alarm set: fxp0 color=RED, class=ETHER,
reason=fxp0: ethernet link down
Jun 11 20:45:07 hissy-re0 mib2d[560]: SNMP_TRAP_LINK_DOWN: ifIndex 1,
ifAdminStatus up(1), ifOperStatus down(2), ifName fxp0
Jun 11 20:45:08 hissy-re0 craftd[556]:  Major alarm set, Connector Interface
Panel Missing
Jun 11 20:45:08 hissy-re0 alarmd[555]: Alarm set: CIP color=RED, class=CHASSIS,
reason=Connector Interface Panel Missing
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match cip command to see specific error messages that are generated when a CIP fails or is offline. Use this information to diagnose a power supply problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display CIP Error Messages in the Chassis Daemon Log File

Action To display CIP error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jun 11 20:45:08 *** inventory change ***
Jun 11 20:45:08 CIP set alarm 0x1
Jun 11 20:45:08 alarm op fru 34 op 1 reason 1
Jun 11 20:45:08 send: red alarm set, class 100 obj 112 reason 1
Jun 11 20:45:08 CIP removed
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Verifying CIP Failure

Steps To Take To verify CIP failure, follow these steps:

1. Check the CIP Connection on page 386
2. Check the Ethernet Port Functionality on page 386
3. Performing a CIP Swap Test on page 387

Step 1: Check the CIP Connection

If the CIP is not seated properly, it will not function.

Action To check the CIP connection, check the screws on the top and bottom of the CIP faceplate and make sure that the CIP is properly seated in the slot.

Step 2: Check the Ethernet Port Functionality

Action To check the Ethernet port, plug an Ethernet cable into the Ethernet port on the CIP.

If the host module is operational, the LINK LED (either the yellow 10-Mbps LED or the green 100-Mbps LED) will flash to register Ethernet activity. If you can run the CLI, the CIP is installed correctly.

Step 3: Performing a CIP Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the CIP for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on a CIP, follow these steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface to receive the CIP.

2. Attach an electrostatic discharge (ESD) strap to your bare wrist and connect the strap to one of the ESD points on the chassis.

3. On the console or other management device connected to each Routing Engine, enter CLI operational mode and issue the following command to shut down the router software. For more information, see the *JUNOS Protocols, Class of Service, System Basics Command Reference*.

   user@host> **request system halt**

   Do not continue until all software processes have shut down.

4. Flip both circuit breaker switches on the circuit breaker box to the OFF (O) position.

5. Disconnect any external devices connected to the CIP.

6. Loosen the screws on the top and bottom of the CIP faceplate.

7. Grasp the CIP and slide it out of the chassis.

8. Check the CIP connector to the router chassis midplane. Look for bent pins.

9. Place the CIP in the electrostatic bag or on the antistatic mat prepared in Step 1.

CAUTION: Be sure to slide the CIP straight out of the slot to avoid damaging the connecting pins on the front of the midplane.

10. Carefully insert the CIP into the left side of the FPC card cage, following the guides on the top and bottom of the card cage.

NOTE: The components on the CIP are on the left side of the board, unlike the components of an FPC, which are on the right side. Verify that the components are on the left before inserting the CIP.

11. Slide the CIP into the chassis until it contacts the midplane.

CAUTION: Be sure to slide the CIP straight into the slot to avoid damaging the connecting pins on the front of the midplane.

12. Tighten the screws on the top and bottom of the CIP faceplate.

13. Reattach any external devices connected to the CIP.

14. Power on the router. See the instructions in the M40e or M160 router hardware guide.

15. To verify that the CIP is installed correctly, plug an Ethernet cable into the CIP port labeled ETHERNET for the appropriate host module.

    When the host module is operational, one of the activity indicator LEDs on the Ethernet port (either the amber 10-Mbps LED or the green 100-Mbps LED) will flash to indicate activity. If you can issue CLI commands over the connection, the CIP is installed correctly.

Getting CIP Hardware Information

Steps To Take To get the CIP hardware information, follow these steps:

1. Display CIP Hardware Information on page 388
2. Locating the CIP Serial Number ID Label on page 389

Step 1: Display CIP Hardware Information

Action To display the CIP hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

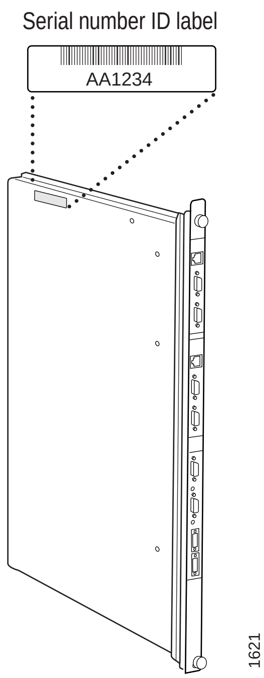
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                51135             M160
[...Output truncated...]
CIP              REV 02   710-001593   AA9564
[...Output truncated...]
```

What It Means The command output displays the CIP slot number, revision level, part number, and serial number.

Step 2: Locating the CIP Serial Number ID Label

Action To locate the CIP serial number ID label, look on the top of the left side of the CIP (see Figure 159).

Figure 159: CIP Serial Number ID Label



Replacing the CIP

The CIP is field-replaceable, but is not hot-removable, hot-insertable, or hot-pluggable. You must power down the router before removing or installing it.

Action To replace a the CIP, see "Return the Failed Component" on page 86, or the procedure to return a field-replaceable unit in the M40e or M160 router hardware guide.

Part 6

Monitoring M40 Internet Router-Specific Components

Chapter 30

Monitoring the SCB

You monitor and maintain the M40 router System Control Board (SCB), the control board for the Packet Forwarding Engine, to ensure that it provides route lookups, system component monitoring, exception and control packet transfer, and Flexible PIC Concentrator (FPC) operation and reset control. (See Table 92.)

Table 92: Checklist for Monitoring the SCB

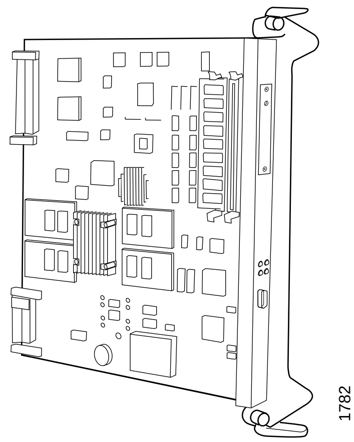
Monitor SCB Tasks	Command or Action
Understanding the SCB on page 394	
Monitoring the SCB Status on page 395	
1. Display the SCB Environmental Status on page 396	show chassis environment
2. Display the SCB Detailed Status on page 396	show chassis scb
3. Check the SCB LED Status on page 397	Check the LEDs on the SCB faceplate.
Checking for SCB Alarms on page 398	
1. Display SCB Error Messages in the System Log File on page 398	show log messages
2. Display SCB Error Messages in the Chassis Daemon Log File on page 399	show log chassisd
Verifying SCB Failure on page 400	
1. Check the SCB Connection on page 400	Ensure that the SCB is securely seated. Tighten the captive screws at the top and bottom of the SCB card carrier.
2. Perform an SCB Swap Test on page 400	Remove the failed SCB and replace it with one that you know works.
Getting SCB Hardware Information on page 401	
1. Display the SCB Hardware Information on page 401	show chassis hardware
2. Locate the SCB Serial Number ID Label on page 402	Look on the front of the SCB board near the faceplate.
3. Display the SCB Firmware Version on page 402	show chassis firmware
Returning the SCB on page 402	See "Return the Failed Component" on page 86, or follow the return procedure in the *M40 Internet Router Hardware Guide*.

Understanding the SCB

Purpose Inspect the SCB, the control board for the Packet Forwarding Engine, to ensure that it provides route lookups, system component monitoring, exception and control packet transfer, and FPC operation and reset control.

What Is the SCB The SCB is the control board for the M40 router Packet Forwarding Engine (see Figure 160).

Figure 160: SCB Component



The SCB performs four major functions:

- Route lookups—The Internet Processor application-specific integrated circuit (ASIC) on the SCB performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM). After performing the lookup, the Internet Processor informs the backplane of the forwarding decision, and the backplane forwards the decision to the appropriate outgoing interface.

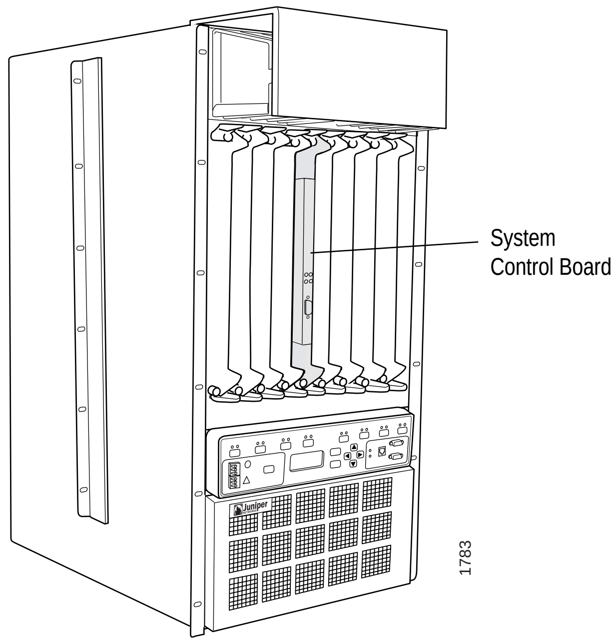
- System component monitoring—The SCB monitors other system components for failure and alarm conditions. It collects statistics from all sensors in the system and relays them to the Routing Engine, which sets the appropriate alarm.

- Exception and control packet transfer—The Internet Processor ASIC on the SCB passes exception packets to a microprocessor on the SCB, which processes almost all of them. The remaining packets are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the SCB are sent to the Routing Engine using SYSLOG messages.

- FPC reset control—The SCB monitors the operation of the FPCs. If it detects errors in an FPC, the SCB attempts to reset the FPC. After three unsuccessful resets, the SCB takes the FPC offline and informs the Routing Engine. Other FPCs are unaffected, and normal system operation continues.

The SCB occupies the center slot of the card cage, and is installed into the backplane from the front of the chassis (see Figure 161).

Figure 161: M40 Router SCB Location



The SCB is field-replaceable and hot-pluggable. You can remove and replace it without powering down the system; however, this causes major impact to the system. While the SCB is out of the router, route lookups, system component monitoring, exception and control packet transfer, and FPC operation and reset control cannot occur.

When you replace the SCB, it is rebooted by flash EEPROM.

Monitoring the SCB Status

If the SCB fails, no information about chassis components is available through the JUNOS software command-line interface (CLI).

Steps To Take To monitor the SCB status, follow these steps:

1. Display the SCB Environmental Status on page 396
2. Display the SCB Detailed Status on page 396
3. Check the SCB LED Status on page 397

Step 1: Display the SCB Environmental Status

Action To display the SCB environment status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                  Status     Measurement
Power Power Supply A        OK
      Power Supply B        Absent
Temp  FPC 0                 OK         29 degrees C / 84 degrees F
      FPC 1                 OK         25 degrees C / 77 degrees F
      FPC 5                 OK         27 degrees C / 80 degrees F
      SCB                   OK         26 degrees C / 78 degrees F
[...Output truncated...]
```

What It Means The command output displays the SCB status and temperature. The SCB status can be OK, Failed, or Absent.

Step 2: Display the SCB Detailed Status

Action To display more detailed SCB status information, use the following CLI command:

user@host> **show chassis scb**

Sample Output

```
user@host> show chassis scb
SCB status:
  Temperature                 27 degrees C / 80 degrees F
  CPU utilization              2 percent
  Interrupt utilization        0 percent
  Heap utilization            16 percent
  Buffer utilization          44 percent
  Total CPU DRAM              64 Mbytes
  Internet Processor II          Version 1, Foundry IBM, Part number 9
  Start time:                    2001-12-07 08:59:04 PST
  Uptime:                        4 hours, 40 minutes, 28 seconds
```

What It Means The command output displays the temperature of the air passing by the SCB, in degrees Centigrade and Fahrenheit. It displays the total percentage of CPU being used by the SCB processor and the percentage being used for interrupts, the percentage of heap space and buffer space being used by the SCB processor, the total DRAM available to the SCB processor, the time when the SCB started running, and how long the SCB has been running. The Internet Processor version and part number are also displayed.

Step 3: Check the SCB LED Status

Action To check the SCB status, look at the LEDs on the SCB faceplate (see Figure 162).

Figure 162: SCB LEDs

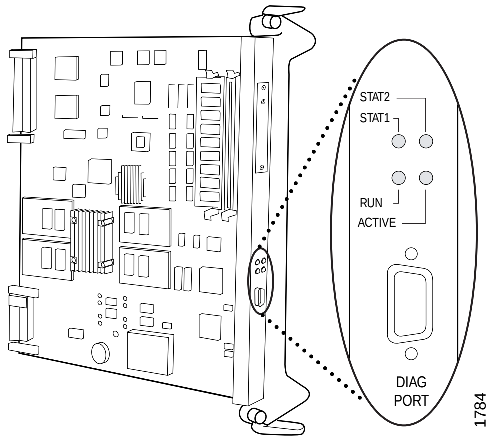


Table 93 describes the SCB LED states.

Table 93: SCB LEDs

Color	Label	State	Description
Green	ACTIVE	Flashing (pulsed with out-time proportional to traffic)	I/O interrupts are occurring.
Green	RUN	Blinking (slow and steady)	SCB processor is running. Normally, the blinking is faint and becomes bright only when the SCB is processing many exceptions.
Amber	STAT1	Flashing	Internal diagnostics are running.
Amber	STAT2	Flashing	Internal diagnostics are running.

If all four SCB LEDs are on, but dimly lit, the SCB is probably not seated properly. Tighten the captive screws at the top and bottom of the SCB card carrier.

If the green RUN LED on the SCB is not blinking, the SCB processor is not functioning normally. The SCB might not be connected properly to the backplane. Tighten the screws at the top and bottom of the SCB card carrier. If that does not work, reinstall the SCB.

The SCB has a reset switch on its faceplate above the LEDs. You normally do not use the reset switch. Pushing the reset switch results in a cold restart of the Packet Forwarding Engine, which causes a service interruption for a minute or two. To trip the reset switch, you must access it through a hole in the faceplate with a paper clip or other small probe.

Checking for SCB Alarms

Steps To Take To check for SCB alarms, follow these steps:

1. Display SCB Error Messages in the System Log File on page 398
2. Display SCB Error Messages in the Chassis Daemon Log File on page 399

Step 1: Display SCB Error Messages in the System Log File

An SCB failure can cause the fpx0 interface, the Ethernet connection to a management LAN, to go up and down.

Action To display SCB error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Nov 19 04:35:29 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:29 host rpd[355]: task_connect: task BGP_209.192.168.0.21+179 addr
192.168.0.21+179: No route to host
Nov 19 04:35:29 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:29 host rpd[355]: bgp_connect_start: connect 192.168.0.21 (Internal
AS 209): No route to host
Nov 19 04:35:29 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:29 host last message repeated 9 times
Nov 19 04:35:29 host tnp.bootpd[369]: BOOTPD_BOOTSTRING: boot 1 scb.jbf
Nov 19 04:35:29 host tnp.tftpd[389]: TFTPD_INFO: tftp read from addr 2 po
rt 1024 file scb.jbf
Nov 19 04:35:31 host tnp.tftpd[389]: TFTPD_INFO: sent 1348 blocks of 1024 and 1
block of 780 for file /usr/share/pfe/scb.jbf
Nov 19 04:35:32 host mgd[387]: UI_CMDLINE_READ_LINE: user 'user', command 'show
chassis scb '
Nov 19 04:35:34 host /kernel: fxp1: link media DOWN 10Mb / half-duplex
Nov 19 04:35:34 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:34 host rpd[355]: EVENT <UpDown> fxp1.0 index 1 <Broadcast
Multicast> address #0 0.80.82.18.14.83
Nov 19 04:35:34 host mib2d[354]: SNMP_TRAP_LINK_DOWN: ifIndex 2, ifAdminStatus
up(1), ifOperStatus down(2), ifName fxp1
Nov 19 04:35:34 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:34 host last message repeated 4 times
Nov 19 04:35:35 host /kernel: fxp1: media DOWN 100Mb / half-duplex
Nov 19 04:35:36 host /kernel: fxp1: link UP 100Mb / half-duplex
Nov 19 04:35:36 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:36 host rpd[355]: EVENT <UpDown> fxp1.0 index 1 <Up Broadcast
Multicast> address #0 0.80.82.18.14.83
Nov 19 04:35:36 host mib2d[354]: SNMP_TRAP_LINK_UP: ifIndex 2, ifAdminStatus
up(1), ifOperStatus up(1), ifName fxp1
Nov 19 04:35:36 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:36 host last message repeated 4 times
Nov 19 04:35:37 host /kernel: fxp1: link media DOWN 10Mb / half-duplex
Nov 19 04:35:37 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
```

```
sendto: No route to host
Nov 19 04:35:37 host rpd[355]: EVENT <UpDown> fxp1.0 index 1 <Broadcast
multicast> address #0 0.80.82.18.14.83
Nov 19 04:35:37 host mib2d[354]: SNMP_TRAP_LINK_DOWN: ifIndex 2, ifAdminStatus
up(1), ifOperStatus down(2), ifName fxp1
Nov 19 04:35:37 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
Nov 19 04:35:37 host last message repeated 4 times
Nov 19 04:35:38 host /kernel: fxp1: media DOWN 100Mb / full-duplex
Nov 19 04:35:38 host /kernel: fxp1: link UP 100Mb / full-duplex
Nov 19 04:35:38 host snmpd[353]: SNMPD_SEND_FAILURE: trap_io_send_trap_now:
sendto: No route to host
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. When the SCB fails, the fxp1 interface keeps going up and down. You can use the show log messages | match scb command to see error messages that are generated when an SCB fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 2: Display SCB Error Messages in the Chassis Daemon Log File

Action To display SCB error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Nov 19 04:09:02 closing alarmd connection.
Nov 19 04:09:02 closing craftd connection.
Nov 19 04:09:02 rcv: chassisd_ipc_dispatch() null ipc_pipe_read, closing connect
ion
Nov 19 04:09:02 alarmd connection completed
Nov 19 04:09:02 craftd connection completed
Nov 19 04:09:30 rcv reply: SCB Restart
Nov 19 04:09:30 send: scb config cmd
Nov 19 04:09:30 send: display hostname <ewr-edge-03>, uptime 16182073 seconds
Nov 19 04:09:30 send: password = nnection.
Nov 19 04:09:30 send: display unlockction.
Nov 19 04:09:30 send: clear all chassis class alarmsc_pipe_read, closing connect
Nov 19 04:09:30 send: set boolean type 0 slot 0 which 1 off
Nov 19 04:09:30 rcv reply: Backplane MAC addrs recieved
Nov 19 04:09:30 rcv reply: Backplane SRAM size 8388608 banks[ 1 1 1 1 ]
Nov 19 04:09:30 jtree init (2097152 4)
Nov 19 04:09:35 repead pid 15567, status 0
Nov 19 04:09:41 rcv reply: chassis info
Nov 19 04:09:49 CHASSISD_EVENT: slot 0 restart
Nov 19 04:09:50 pic online req, pic 0 type 515, fpc 0
Nov 19 04:09:50 send: fpc 0 pic 0 online ack
Nov 19 04:09:51 CHASSISD_EVENT: slot 0 attach
Nov 19 04:09:51 rcv reply: PIC attach fpc 0 pic 0 type 515 version 260
Nov 19 04:09:52 CHASSISD_EVENT: slot 1 restart
Nov 19 04:09:53 pic online req, pic 0 type 515, fpc 1
Nov 19 04:09:53 send: fpc 1 pic 0 online ack
Nov 19 04:09:54 CHASSISD_EVENT: slot 2 restart
Nov 19 04:09:55 pic online req, pic 0 type 518, fpc 2
Nov 19 04:09:55 send: fpc 2 pic 0 online ack
Nov 19 04:09:55 pic online req, pic 1 type 518, fpc 2
```

```
Nov 19 04:09:55 send: fpc 2 pic 1 online ack
Nov 19 04:09:55 pic online req, pic 2 type 518, fpc 2  515 version 260
Nov 19 04:09:55 send: fpc 2 pic 2 online ackrt
Nov 19 04:09:57 CHASSISD_EVENT: slot 3 restart, fpc 1
Nov 19 04:09:58 CHASSISD_EVENT: slot 4 restart
Nov 19 04:09:58 CHASSISD_EVENT: slot 1 attach
Nov 19 04:09:59 pic online req, pic 0 type 518, fpc 4
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the chassisd log file by using the | match "item | item | item" command. For example, | match "scb | kernel | tnp" is a search for error messages for the SCB, kernel, and Trivial Networking Protocol (TNP), and indicates communication issues between the Routing Engine and the Packet Forwarding Engine components.

Verifying SCB Failure

Steps To Take To verify SCB failure, follow these steps:

1. Check the SCB Connection on page 400
2. Perform an SCB Swap Test on page 400

Step 1: Check the SCB Connection

If the SCB is not seated properly, it will not function.

Action To check the SCB connection, make sure that the SCB is properly seated in the slot. Tighten the captive screws at the top and bottom of the SCB card carrier.

Step 2: Perform an SCB Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SCB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an SCB, follow these steps:

1. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
2. Unscrew the thumbscrews at the top and bottom of the card carrier.
3. Flip the ends of the two extractor clips, which are adjacent to the thumbscrews, away from each other to unseat the SCB from the backplane.
4. Grasp both sides of the card carrier and slide the SCB about three-quarters of the way out of the router.
5. Move one of your hands underneath the SCB to support it, and slide it completely out of the chassis.

6. Replace the SCB with one that you know works.
7. Grasp the front of the SCB card carrier with both hands and align the back of the working SCB card carrier with the slide guides on the chassis.
8. Slide the SCB card carrier all the way into the card cage until it contacts the backplane.
9. Flip the extractor clips, located on the top and bottom of the card carrier, towards each other to lodge the SCB in place.
10. Tighten the thumbscrews on the card carrier to seat the SCB.

NOTE: To seat the SCB properly, be sure to tighten the screws securely. If the SCB is not seated properly, it will not function.

Getting SCB Hardware Information

Steps To Take To obtain SCB hardware information, follow these steps:

1. Display the SCB Hardware Information on page 401
2. Locate the SCB Serial Number ID Label on page 402
3. Display the SCB Firmware Version on page 402

Step 1: Display the SCB Hardware Information

Action To display the SCB hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

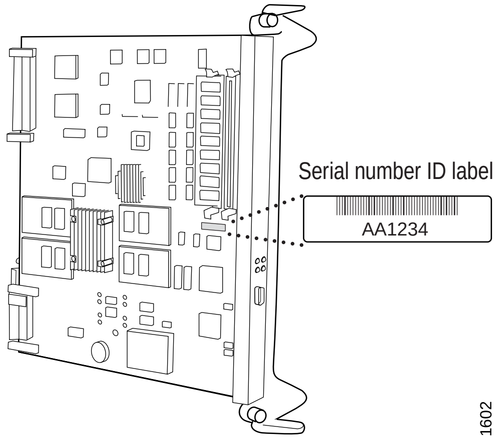
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                00291             M40
Backplane        REV 10   710-000073   AA2220
Power Supply A   Rev A1   740-000234   000134            AC
Maxicab          REV 07   710-000229   AA6957
Minicab          REV 03   710-000482   AA3324
Display          REV 07   710-000150   AA7798
Routing Engine                                           RE-1.0
SCB              REV 11   710-000075   AA7244            Internet Processor I
[...Output truncated...]
```

What It Means The command output displays the SCB version level, part number, serial number, and description.

Step 2: Locate the SCB Serial Number ID Label

Action To locate the SCB serial number ID label, look on the SCB board toward the front panel.

Figure 163: SSB Serial Number ID Label



Step 3: Display the SCB Firmware Version

Action To display the version of firmware running on the SCB, use the following CLI command:

user@host> **show chassis firmware**

Sample Output

```
user@host> show chassis firmware
Part                    Type       Version
[...Output truncated...]
SCB 0                   ROM        Juniper ROM Monitor Version 3.0b1
                        O/S        Version 5.5-20020613-cqPqI7 by builder on 2
```

What It Means The command output displays the type and version level of the firmware running on the SCB.

Returning the SCB

The SCB is field-replaceable and hot-pluggable. You can remove and replace it without powering down the system; however this causes major impact to the system. While the SCB is out of the router, route lookups, system component monitoring, exception and control packet transfer, and FPC operation monitoring cannot occur.

Action To return the SCB, see “Return the Failed Component” on page 86, or the return procedure in the *M40 Internet Router Hardware Guide*.

Part 7

Monitoring M20 Internet Router-Specific Components

Chapter 31

Monitoring the SSB

You monitor the M20 router System and Switch Board (SSB) to ensure that it provides allocation of incoming data packets throughout shared memory on the Flexible PIC Concentrators (FPCs), transfers outgoing data cells to the FPCs for packet reassembly, performs route lookups using the forwarding table, monitors system components for failure and alarm conditions, and monitors FPC operation and reset. (See Table 94.)

Table 94: Checklist for Monitoring the SSB

Monitor SSB Tasks	Command or Action
Understanding the SSB on page 406	
Monitoring the SSB Status on page 408	
1. Display the SSB Environmental Status on page 408	show chassis environment
2. Display the SSB Detailed Status on page 409	show chassis ssb
3. Check the SSB LEDs on page 409	Check the LEDs on the SCB faceplate.
Checking for SSB Alarms on page 410	
1. Display SSB Error Messages in the System Log File on page 410	show log messages
2. Display SSB Error Messages in the Chassis Daemon Log File on page 411	show log chassisd | match ssb
Verifying SSB Failure on page 411	
1. Check the SSB Connection on page 411	Check the thumbscrews on the left and right sides of the SSB.
2. Perform a Swap Test on the SSB on page 412	1. Take the SSB offline. 2. Remove the SSB. 3. Replace the SSB with one that you know works.
Getting SSB Hardware Information on page 413	
1. Display the SSB Hardware Information on page 413	show chassis hardware
2. Locate the SSB Serial Number ID Label on page 413	Look for the SSB serial number label located on the top of the SSB adjacent to the SDRAM memory bank.
3. Display the SSB Firmware Version on page 414	show chassis firmware
Replacing the SSB on page 414	See "Return the Failed Component" on page 86, or follow the procedure in the *M20 Internet Router Hardware Guide*.

Understanding the SSB

Purpose Inspect the SSB to ensure that it provides allocation of incoming data packets throughout shared memory on the FPCs, transfers outgoing data cells to the FPCs for packet reassembly, performs route lookups using the forwarding table, monitors system components for failure and alarm conditions, and monitors FPC operation and reset.

What Is the SSB The SSB is a component of the Packet Forwarding Engine and performs the following major functions (see Figure 164 on page 407):

- Shared memory management on the FPCs—The Distributed Buffer Manager application-specific integrated circuit (ASIC) on the SSB uniformly allocates incoming data packets throughout shared memory on the FPCs.

- Outgoing data cell transfer to the FPCs—A second Distributed Buffer Manager ASIC on the SSB passes data cells to the FPCs for packet reassembly when the data is ready to be transmitted.

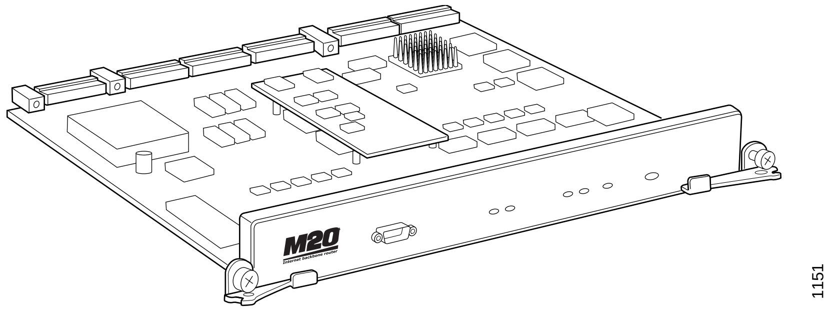
- Route lookups—The Internet Processor ASIC on the SSB performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM). After performing the lookup, the Internet Processor ASIC informs the midplane of the forwarding decision, and the midplane forwards the decision to the appropriate outgoing interface.

- System component monitoring—The SSB monitors other system components for failure and alarm conditions. It collects statistics from all sensors in the system and relays them to the Routing Engine, which sets the appropriate alarm. For example, if a temperature sensor exceeds the first internally defined threshold, the Routing Engine issues a “high temp” alarm. If the sensor exceeds the second threshold, the Routing Engine initiates a system shutdown.

- Exception and control packet transfer—The Internet Processor ASIC passes exception packets to a microprocessor on the SSB, which processes almost all of them. The remaining packets are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the SSB are sent to the Routing Engine using system log messages.

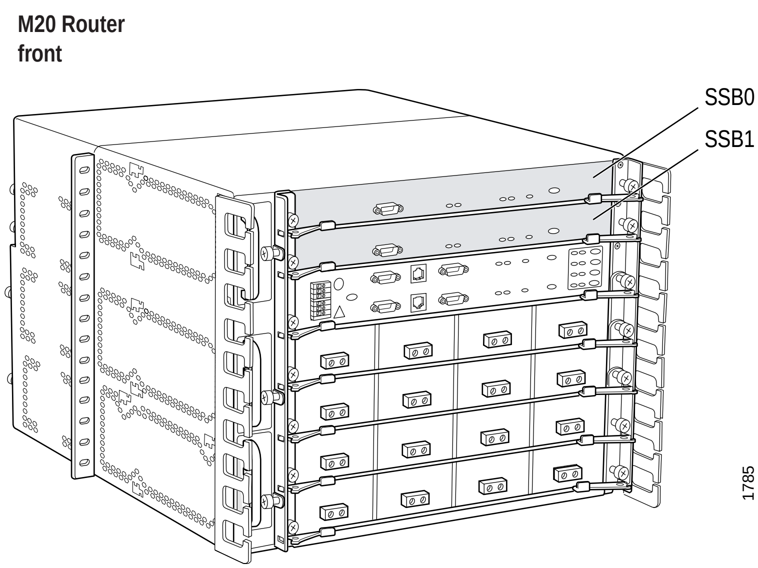
- FPC reset control—The SSB monitors the operation of the FPCs. If it detects errors in an FPC, the SSB attempts to reset the FPC. After three unsuccessful resets, the SSB takes the FPC offline and informs the Routing Engine. Other FPCs are unaffected, and normal system operation continues.

Figure 164: SSB Component



You can install two SSBs in the M20 router. The SSBs occupy the two top slots of the card cage (SSB0 and SSB1), and are installed into the midplane from the front of the chassis. (See Figure 165.)

Figure 165: M20 Router SSB Location



The SSB houses the Internet Processor ASIC and two Distributed Buffer Manager ASICs.

The SSB is hot-pluggable. You can remove and replace it without powering down the system; however, this causes major impact to the system. While the SSB is out of the router, route lookups, system component monitoring, exception and control packet transfer, and FPC resets cannot occur.

When the SSB is removed, all packet forwarding stops immediately and the Routing Engine responds by generating alarms. When the SSB is replaced, it is rebooted by flash EEPROM.

If you have removed the Routing Engine, the SSB enters a warm shutdown mode and continues its forwarding process for a limited time using a frozen forwarding table. The time limit is determined by a timer in the SSB. If you replace the Routing Engine during the warm shutdown period, the SSB unfreezes its forwarding tables and resumes normal functioning. Otherwise, the SSB shuts down.

Monitoring the SSB Status

If the SSB fails, no information about the chassis components is available through the JUNOS software command-line interface (CLI).

Steps To Take To monitor the SSB, follow these steps:

1. Display the SSB Environmental Status on page 408
2. Display the SSB Detailed Status on page 409
3. Check the SSB LEDs on page 409

Step 1: Display the SSB Environmental Status

Action To display the SSB environmental status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                  Status     Measurement
Power Power Supply A        Failed
      Power Supply B        OK
Temp  FPC Slot 0            OK         27 degrees C / 80 degrees F
      FPC Slot 1            OK         30 degrees C / 86 degrees F
      FPC Slot 2            OK         26 degrees C / 78 degrees F
      FPC Slot 3            OK         25 degrees C / 77 degrees F
      Power Supply A        OK         28 degrees C / 82 degrees F
      Power Supply B        OK         24 degrees C / 75 degrees F
      SSB Slot 0            OK         25 degrees C / 77 degrees F
      Backplane             OK         21 degrees C / 69 degrees F
Fans  Rear Fan              OK         Spinning at normal speed
      Upper Fan             OK         Spinning at normal speed
      Middle Fan            OK         Spinning at normal speed
      Bottom Fan            OK         Spinning at normal speed
Misc  Craft Interface       OK
```

What It Means The command output displays the SSB status and temperature. The SSB status can be OK, Failed, or Absent.

Step 2: Display the SSB Detailed Status

Action To display more detailed SSB status information, use the following CLI command:

user@host> **show chassis ssb**

Sample Output

```
user@host> show chassis ssb
SSB status:
  Failover:                     0 time
  Slot 0:
    State:                        Master
    Temperature:               33 Centigrade
    CPU utilization:            0 percent
    Interrupt utilization:      0 percent
    Heap utilization:           0 percent
    Buffer utilization:         6 percent
    DRAM:                      64 Mbytes
    Start time:                   1999-01-15 22:05:36 UTC
    Uptime:                       21 hours, 21 minutes, 22 seconds
  Slot 1:
    State:                        Backup
```

What It Means The command output displays the number of times the mastership has changed, the SSB slot number 0 or 1, and the current state of the SSB: Master, Backup, or Empty. The command output displays the temperature of the air passing by the SSB, in degrees Centigrade. It also displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the SSB processor, including the total DRAM available to the SSB processor. The command output displays the time when the SSB started running and how long the SSB has been running.

Alternative Action To display the status for a particular SSB, use the following CLI command:

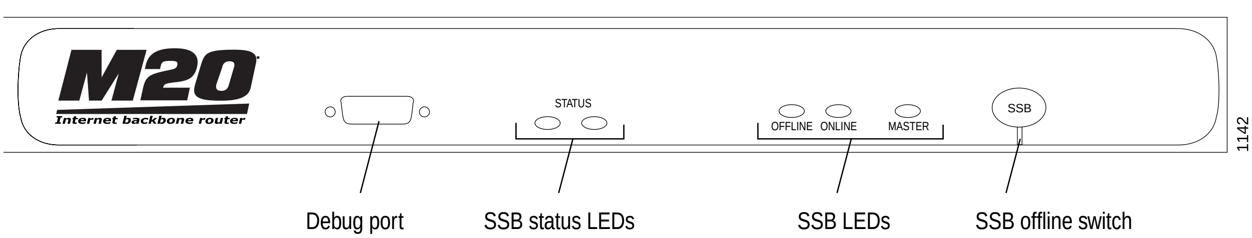
user@host> **show chassis ssb** *slot*

Step 3: Check the SSB LEDs

Periodically check the SSB LEDs to verify that the SSB is online or offline and the type of task it is performing.

Action To check the SSB LEDs, look on the faceplate at the front of the router (see Figure 166).

Figure 166: SSB LEDs



The SSB has two groups of LEDs: online/offline LEDs and status LEDs. The online/offline LEDs indicate whether the SSB is online or offline. The status LEDs indicate what type of task the SSB is performing. Table 95 describes the LED states.

Table 95: SSB LEDs

Label	Color	State	Description
OFFLINE	Amber	On steadily	SSB is offline.
ONLINE	Green	On steadily	SSB processor is running.
MASTER	Blue	On steadily	SSB is master.
STATUS (left)	Green	Blinking	SSB processor is running. Normally, the blinking is faint and becomes bright only when the SSB is processing many exceptions.
STATUS (right)	Green	Flashing	I/O interrupts are occurring.

Checking for SSB Alarms

Steps To Take To check for SSB alarms, follow these steps

1. Display SSB Error Messages in the System Log File on page 410
2. Display SSB Error Messages in the Chassis Daemon Log File on page 411

Step 1: Display SSB Error Messages in the System Log File

Periodically check the SYSLOG messages on the management console for messages sent by the SSB. During normal operation, the SSB notifies the Routing Engine of any errors it detects.

Action To display the SSB error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 100Mb / full-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 10Mb / half-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 100Mb / full-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: link UP 100Mb / full-duplex
Jul 10 13:28:45 myrouter rpd[564]: EVENT <UpDown> fxp1.0 index 1 <Up Broadcast
Multicast> address #0 0.a0.a5.12.1d.6d
Jul 10 13:28:45 myrouter mib2d[563]: SNMP_TRAP_LINK_UP: ifIndex 2, ifAdminStatus
up(1), ifOperStatus up(1), ifName fxp1
[...Output truncated...]
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match ssb command to see error messages that are generated when an SSB fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what the error messages are and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 2: Display SSB Error Messages in the Chassis Daemon Log File

Action To display the SSB error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd | match ssb**

Sample Output

```
user@host> show log chassisd |match ssb
Jul 10 13:27:28 SSB0 is now not present
Jul 10 13:27:28 Assert reset on SSB0
Jul 10 13:27:28 Turn on ethernet loop
[...Output truncated...]
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the chassisd log file by using the | match "item | item | item" command. For example, | match "ssb | kernel | tnp" is a search for error messages for the SSB, kernel, and Trivial Networking Protocol (TNP), and indicates communication issues between the Routing Engine and the Packet Forwarding Engine components.

Verifying SSB Failure

Steps To Take To verify SSB failure, follow these steps:

1. Check the SSB Connection on page 411
2. Perform a Swap Test on the SSB on page 412

Step 1: Check the SSB Connection

If the SSB is not seated properly, it will not function.

Action To check the SSB connection, make sure that the SSB is properly seated in the slot. To seat the SSB properly, securely tighten the screws on the left and right sides of the card carrier.

Step 2: Perform a Swap Test on the SSB

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SSB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an SSB, follow these steps:

1. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
2. Locate the SSB offline switch on the front panel and press and hold the switch for 5 seconds to take the SSB offline.

CAUTION: If you take the SSB offline, packet forwarding will be affected.

3. Unscrew the thumbscrews on the left and right sides of the card carrier to unseat the SSB from the midplane.
4. Flip the ends of the two extractor clips, which are adjacent to the thumbscrews, towards the outside edges of the router.
5. Grasp both sides of the card carrier and slide the SSB about three-quarters of the way out of the router.
6. Move one of your hands underneath the SSB to support it, and slide it completely out of the chassis.
7. Replace the SSB with one that you know works.
8. Grasp the front of the SSB card carrier with both hands and align the back of the card carrier with the slide guides on the chassis.
9. Slide the SSB card carrier all the way into the card cage until it contacts the midplane.
10. Flip the extractor clips, located on the left and right sides of the card carrier, towards each other to secure the SSB in place.
11. Tighten the thumbscrews on the left and right sides of the card carrier to seat the SSB.

NOTE: To seat the SSB properly, be sure to tighten the screws securely. If the SSB is not seated properly, it will not function.

Getting SSB Hardware Information

Steps To Take

1. Display the SSB Hardware Information on page 413
2. Locate the SSB Serial Number ID Label on page 413
3. Display the SSB Firmware Version on page 414

Step 1: Display the SSB Hardware Information

Action To display the SSB hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

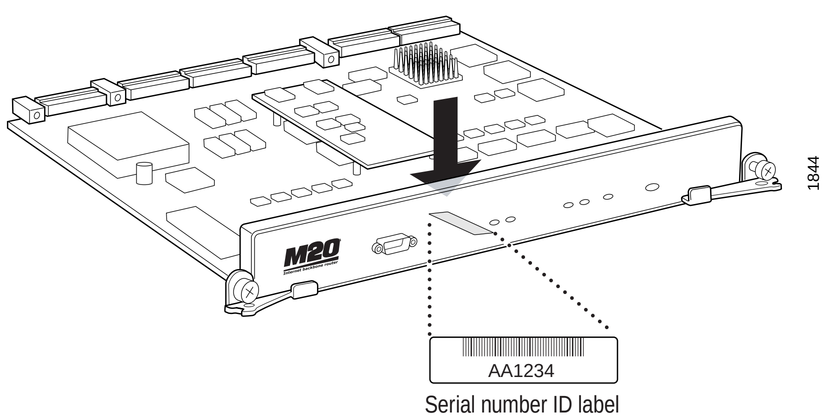
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
[...Output truncated...]
SSB slot 0       REV 01   710-001951   AD5904            Internet Processor II
SSB slot 1       N/A      N/A          N/A               backup
[...Output truncated...]
```

What It Means The command output displays the SSB version level, part number, serial number, and description.

Step 2: Locate the SSB Serial Number ID Label

Action To locate the SSB serial number ID label, look on the top of the SSB adjacent to the SDRAM memory bank.

Figure 167: SSB Serial Number ID Label



Step 3: Display the SSB Firmware Version

Action To display the version of firmware running on the SSB, use the following CLI command:

user@host> **show chassis firmware**

Sample Output

```
user@host> show chassis firmware
Part                     Type       Version
[...Output truncated...]
SSB 0                    ROM        Juniper ROM Monitor Version 4.2b1
                         O/S        Version 5.4I20020626_0216_mtiwari by mtiwar
SSB 1
```

What It Means The command output displays the type and version level of the firmware running on the SSB.

Replacing the SSB

The SSB is hot-pluggable. When the SSB is removed, all packet forwarding stops immediately and the Routing Engine responds by sending alarms through the Ethernet channel to the management console. When the SSB is replaced, it is rebooted by flash EEPROM.

Action If the SSB fails, replace it as described in the *M20 Internet Router Hardware Guide*.

Part 8

Monitoring M7i and M10i Router-Specific Components

Chapter 32

Monitoring the CFEBs

You monitor the Compact Forwarding Engine Board (CFEB), which provides route lookup, filtering, and switching on incoming data packets, then directs outbound packets to the appropriate interface for transmission to the network. (See Table 96.)

The M7i router CFEB can process 8 million packets per second (Mpps); the M10i router CFEB can process 16 Mpps.

The CFEB communicates with the Routing Engine using a dedicated 100-Mbps Fast Ethernet link that transfers routing table data from the Routing Engine to the forwarding table in the integrated ASIC. The link is also used to transfer from the CFEB to the Routing Engine routing link-state updates and other packets destined for the router that have been received through the router interfaces.

Table 96: Checklist for Monitoring the CFEB

Monitor CFEB Tasks	Command or Action
Understanding the CFEB on page 419	
■ M7i Router CFEB on page 419 ■ M7i Router CFEB with ASP-I on page 420 ■ M10i Router CFEB Component on page 421 ■ M7i and M10i Router CFEB Location on page 421	
Monitoring the CFEB Status on page 421	
1. Display the CFEB Environmental Status on page 422	show chassis environment
2. Display the CFEB Detailed Status on page 422	show chassis cfeb
3. Check CFEB LEDs on page 423	Look at the LEDs on the CFEB faceplate located on the rear of the router above the power supplies.
Checking for CFEB Alarms on page 423	
1. Display CFEB Alarms on page 423	show chassis alarms (M7i router) Look at the alarm LEDs on the right side of the Fixed Interface Card (FIC). (M10i router) Look at the alarm LEDs on the right side of the High-Availability Chassis Manager (HCM). For a listing of the conditions that trigger CFEB alarms, see "M7i or M10i Router Chassis Component Alarm Conditions" on page 63.
2. Check the CFEB LEDs on page 424	Look at the three LEDs located on the component faceplate. The CFEB is located on the rear of the router above the power supplies.

Monitor CFEB Tasks	Command or Action
3. Display CFEB Error Messages in the System Log File on page 424	show log messages | match cfeb
4. Display CFEB Error Messages in the Chassis Daemon Log File on page 425	show log chassisd | match cfeb
Verifying CFEB Failure on page 426	
1. Check the CFEB Uptime on page 426	show chassis cfeb
2. Check the System Uptime on page 427	show system uptime
3. Check the CFEB Connection on page 427	Check that the thumbscrews on each CFEB ejector lever are securely tightened.
4. Perform a Swap Test on the CFEB on page 427	■ Before performing a swap test, always check for bent pins in the midplane and check the CFEB for stuck pins in the connector. ■ Power down the CFEB before removing it by pressing and holding down the offline button on the faceplate until the amber LED labeled FAIL lights, or by using the request chassis cfeb offline CLI command. ■ Power up the CFEB after installing it by pressing and holding down the offline button on the CFEB faceplate until the green LED labeled Output OK lights steadily, or by using the request chassis cfeb online CLI command. ■ Follow the procedure in the appropriate router hardware guide for replacing and installing a CFEB.
Getting CFEB Hardware Information on page 429	
1. Display the CFEB Hardware Information on page 429	show chassis hardware
2. Display the CFEB Firmware Information on page 430	show chassis firmware
3. Locate the CFEB Serial Number ID Label on page 430	Look on the right side of the CFEB top panel.
Returning the CFEB on page 430	See "Return the Failed Component" on page 86 or follow the procedure in the appropriate router hardware guide.

Understanding the CFEB

Purpose Monitor the CFEB so that it can provide route lookup, filtering, and switching on incoming data packets and direct outbound packets to the appropriate interface for transmission to the network.

What Is an CFEB The CFEB processes 16 Mpps. The CFEB performs the following functions:

- Route lookups—Performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM).
- Management of shared memory —Uniformly allocates incoming data packets throughout the router's shared memory.
- Transfer of outgoing data packets—Passes data packets to the destination FIC or Physical Interface Card (PIC) when the data is ready to be transmitted.
- Transfer of exception and control packets—Passes exception packets to the microprocessor on the CFEB, which processes almost all of them. The remainder are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the CFEB are sent to the Routing Engine using system log messages.
- (M7i router only) Built-in tunnel interface—Encapsulates arbitrary packets inside a transport protocol, providing a private, secure path through an otherwise public network.

  The built-in tunnel interface on the CFEB is configured the same way as a PIC. For information about configuring the built-in tunnel interface, see the *JUNOS Services Interfaces Configuration Guide*.
- (M7i router only) Optional Adaptive Services PIC–Integrated (ASP–I)—Provides one or more services on one PIC. See "Adaptive Services PIC–Integrated (ASP–I)" on page 11 for more information.

Figure 168 shows the M7i router CFEB component.

Figure 168: M7i Router CFEB

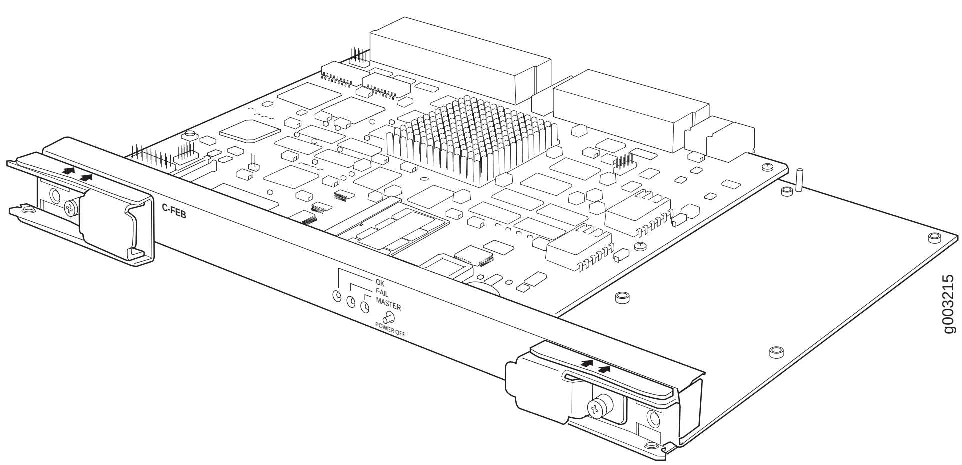
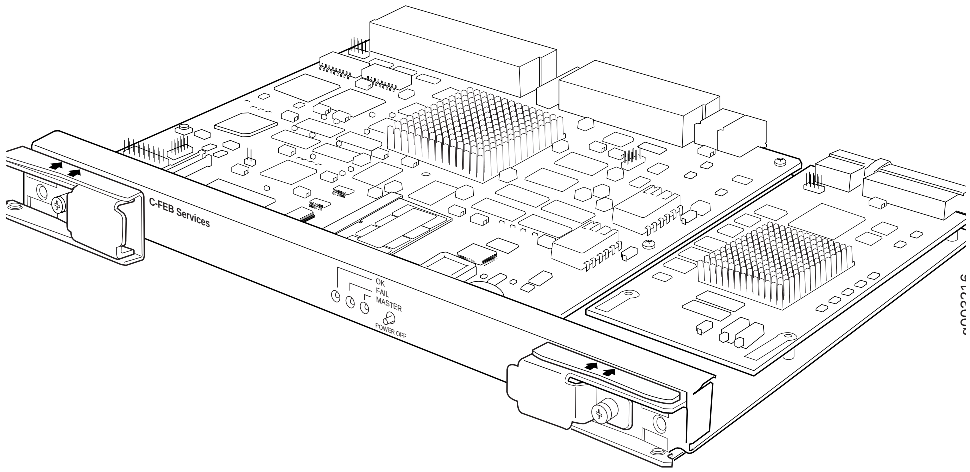


Figure 169 shows the M7i router CFEB with ASP-I.

Figure 169: M7i Router CFEB with ASP-I



The ASP–I is an optional component of the CFEB. The ASP–I is similar to the standalone Adaptive Services PIC, but operates at a reduced bandwidth. The ASP–I enables you to perform one or more services on the same PIC by configuring a set of services and applications.

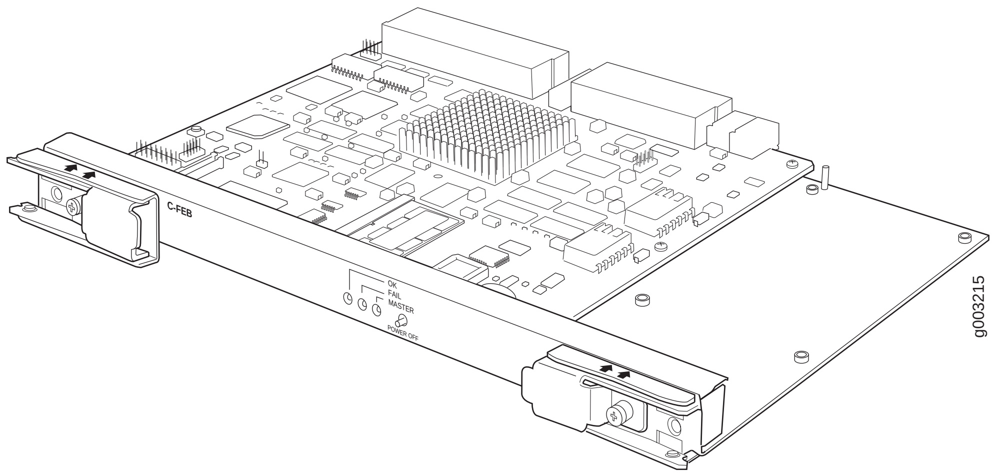
The ASP–I provides the following services:

- Stateful firewall—A type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic.
- Network Address Translation (NAT)—A security procedure for concealing host addresses on a private network behind a pool of public addresses.
- Intrusion detection services (IDS)—A set of tools for detecting, redirecting, and preventing certain kinds of network attack and intrusion.

The configuration for these three services comprises a series of rules that you can arrange in order of precedence as a rule set. Each rule follows the structure of a firewall filter, with a from statement containing input or match conditions and a then statement containing actions to be taken if the match conditions are met. For information about configuring interfaces on the ASP–I, see the *JUNOS Services Interfaces Configuration Guide*.

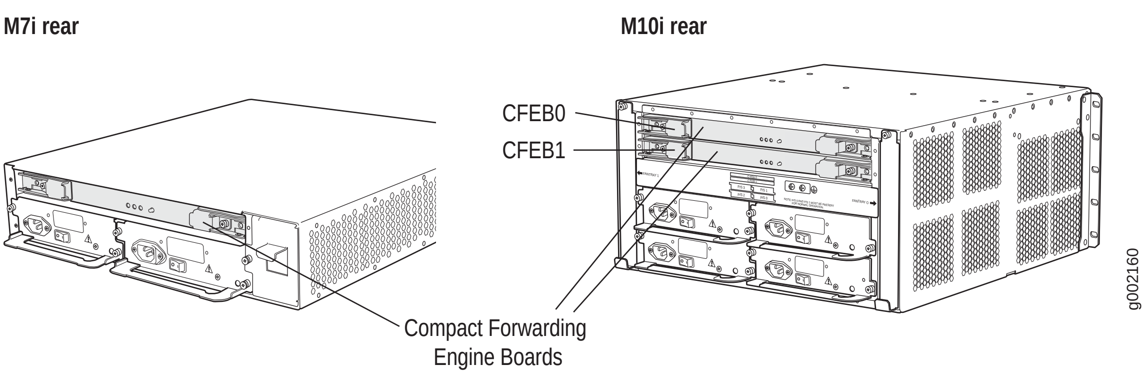
Figure 170 shows the M10i router CFEB component.

Figure 170: M10i Router CFEB Component



You can install one CFEB in the M7i router from the rear of the router above the power supplies. You can install one or two CFEBs from the rear of the M10i router chassis above the fan tray (see Figure 171).

Figure 171: M7i and M10i Router CFEB Location



Monitoring the CFEB Status

Steps To Take To monitor the CFEB status, follow these steps:

1. Display the CFEB Environmental Status on page 422
2. Display the CFEB Detailed Status on page 422
3. Check CFEB LEDs on page 423

Step 1: Display the CFEB Environmental Status

Action To display the CFEB environmental status, use the following command-line interface (CLI) command:

user@host> **show chassis environment**

Sample Output

```
user@m5-host> show chassis environment
Class Item                   Status     Measurement
Power Power Supply 0         OK
      Power Supply 1         Absent
Temp  Intake                 OK         22 degrees C / 71 degrees F
      FPC 0                  OK         23 degrees C / 73 degrees F
      Power Supplies         OK         23 degrees C / 73 degrees F
      CFEB Intake            OK         24 degrees C / 75 degrees F
      CFEB Exhaust           OK         30 degrees C / 86 degrees F
[...Output truncated...]
```

What It Means The command output displays the temperature and status of the CFEB intake and exhaust, which can be OK, Failed, or Absent.

Step 2: Display the CFEB Detailed Status

Action To display more detailed CFEB status, use the following CLI command:

user@host> **show chassis cfeb**

Sample Output

```
user@host> show chassis cfeb
CFEB status:
Slot 0 information:
  State                                 Master
  Intake temperature                 29 degrees C / 84 degrees F
  Exhaust temperature                38 degrees C / 100 degrees F
  CPU utilization                     3 percent
  Interrupt utilization               0 percent
  Heap utilization                   10 percent
  Buffer utilization                 22 percent
  Total CPU DRAM                    128 MB
  Internet Processor II                 Version 1, Foundry IBM, Part number 164
  Start time:                           2004-09-28 03:07:54 PDT
  Uptime:                              9 days, 18 hours, 36 minutes, 15 seconds
Slot 1 information:
  State                                 Backup
```

What It Means The command output displays the temperature of the air passing by the CFEB intake and exhaust, in degrees Centigrade. It displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the CFEB processor, including the total DRAM available to the CFEB processor. The command output displays the time when the CFEB started running and how long the CFEB has been running. A short uptime can indicate that there is a CFEB problem.

Step 3: Check CFEB LEDs

Three LEDs—a green LED labeled OK, a red LED labeled FAIL, and a blue LED labeled MASTER—indicate CFEB status.

Action Look at the LEDs on the CFEB faceplate. The CFEB is located on the rear of the router above the power supplies (see Figure 171 on page 421). Table 97 describes the CFEB LED states.

Table 97: CFEB LEDs

Label	Color	State	Description
OK	Green	On steadily	CFEB is running normally.
		Blinking	CFEB is starting up.
FAIL	Red	On steadily	CFEB is not operational or is in reset mode.
MASTER	Blue	On steadily	CFEB is functioning as master.

Checking for CFEB Alarms

For a listing of the conditions that trigger CFEB alarms, see “M7i or M10i Router Chassis Component Alarm Conditions” on page 63.

Steps To Take To check for CFEB alarms, follow these steps:

1. Display CFEB Alarms on page 423
2. Check the CFEB LEDs on page 424
3. Display CFEB Error Messages in the System Log File on page 424
4. Display CFEB Error Messages in the Chassis Daemon Log File on page 425

Step 1: Display CFEB Alarms

For conditions that trigger CFEB alarms, see “Display the Current Router Alarms” on page 61.

Action To display CFEB alarms, use the following CLI command:

user @host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarms currently active
Alarm time              Class  Description
2004-10-08 00:29:02 PDT  Major  CFEB not online, the box is not forwarding
```

What It Means The command output displays the alarm date, time, severity level, and description.

Alternative Action The CFEB generates a red alarm. Table 98 displays the CFEB alarms, severity, and remedies.

Table 98: CFEB Alarms, Remedies, and Severity

Chassis Compoment	Alarm Condition	Remedy	Alarm Severity
CFEB	The router has an optional internal flash drive and boots from an alternate boot device. If you configure your router to boot from the hard disk, ignore this alarm condition.	Replace the failed or missing CFEB.	Red
	Both CFEBs have been removed or have failed.	Replace the failed or missing CFEB.	Red
	Too many hard errors in CFEB memory.	Replace fthe ailed CFEB.	Red
	A CFEB microcode download has failed.	Replace the failed CFEB.	Red

(M7i router) Look at the alarm LEDs on the right side of the FIC.

(M10i router) Look at the alarm LEDs on the right side of the HCM.

Step 2: Check the CFEB LEDs

Action To check the CFEB LEDs, see “Check CFEB LEDs” on page 423.

Table 99: CFEB LEDs

Label	Color	State	Description
OK	Green	On steadily	CFEB is running normally.
		Blinking	CFEB is starting up.
FAIL	Red	On steadily	CFEB is not operational or is in reset mode.
MASTER	Blue	On steadily	CFEB is functioning as master.

Step 3: Display CFEB Error Messages in the System Log File

Check for messages at least 5 minutes before and after a CFEB alarm occurs.

Action To check for CFEB error messages in the system log messages file, use the following CLI command:

user@host> **show log messages | match cfeb**

Sample Output

```
user@host> show log messages | match cfeb
Sep 14 11:00:01  clinton cfeb CM: ALARM SET: (Major) Slot 0: CFEB not online,
the box is not forwarding
Sep 14 11:00:11  clinton craftd[4896]: Major alarm cleared, CFEB not online, the
box is not forwarding
Sep 14 11:00:11  clinton alarmd[4893]: Alarm cleared: CFEB color=RED, class=
CHASSIS, reason=CFEB not online, the box is not forwarding
Sep 14 11:00:12  clinton cfeb CM: ALARM CLEAR: Slot 0: CFEB not online, the box
is not forwarding
Oct  8 00:29:02  clinton craftd[4896]:  Major alarm set, CFEB not online, the
```

```
box is not forwarding
Oct  8 00:29:02  clinton chassisd[4891]: CHASSISD_SHUTDOWN_NOTICE: Shutdown
reason: CFEB connection lost
Oct  8 00:29:02  clinton alarmd[4893]: Alarm set: CFEB color=RED, class=CHASSIS,
reason=CFEB not online, the box is not forwarding
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match cfeb command to see error messages that are generated when a Control Board fails or is offline. Use this information to diagnose a Control Board problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 4: Display CFEB Error Messages in the Chassis Daemon Log File

Action To display CFEB error messages in the chassisd log file, use the following CLI command:

user@host> **show log chassisd | match cfeb**

Sample Output

```
user@host> show log chassisd | match cfeb
Apr 28 03:25:13 Resetting CFEB 0
Apr 28 03:25:26 send: red alarm set, device CFEB 0, reason CFEB Not Online
Apr 28 03:25:26 Resetting CFEB 0
Apr 28 03:25:27 CFEB 0 added
Apr 28 03:25:27 CHASSISD_SNMP_TRAP7: SNMP trap generated: FRU insertion (jnxFruC
ontentsIndex 6, jnxFruL1Index 1, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName
CFEB, jnxFruType 4, jnxFruSlot 1)
Apr 28 03:25:46 Resetting CFEB 0
Apr 28 03:28:42 send: red alarm set, device CFEB 0, reason CFEB Not Online
Apr 28 03:28:42 Resetting CFEB 0
Apr 28 03:28:43 CFEB 0 added
Apr 28 03:28:43 CHASSISD_SNMP_TRAP7: SNMP trap generated: FRU insertion (jnxFruC
ontentsIndex 6, jnxFruL1Index 1, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName
CFEB, jnxFruType 4, jnxFruSlot 1)
Apr 28 03:29:17 rcv reply: CFEB Restart
Apr 28 03:29:17 CHASSISD_SNMP_TRAP9: SNMP trap generated: FRU power on (jnxFruCo
ntentsIndex 6, jnxFruL1Index 1, jnxFruL2Index 0, jnxFruL3Index 0, jnxFruName
CFEB, jnxFruType 4, jnxFruSlot 1, jnxFruOfflineReason 2, jnxFruLastPowerOff
5526, jnxFruLastPowerOn 5526)
Apr 28 03:29:17 sending 1 queued messages to CFEB 0
Apr 28 03:29:17 missing ctm for CFEB 0 -- timerid 0x0, timerset 0
Apr 28 03:29:17 send: CFEB config cmd
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting debugmode off
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting coredump on
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting source-route on
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting mtu-check off
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting soft-restart on
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting pfeman-reconnect off
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting l2cache on
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting no-load-balancing-clone off
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting equal-weighted-mode off
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting ipv4-key-hash-L3 on
Apr 28 03:29:17 send: set_boolean_cmd CFEB 0 setting mpls-key-hash-2label off
Apr 28 03:29:27 send: red alarm clear, device CFEB 0, reason CFEB Not Online
```

What It Means The **chassisd** database provides the date, time, and a component status message. The **chassisd** database is dynamic. It is initialized at router startup and is updated when components are added or removed. You can search for multiple items in the **chassisd** log file by using the **show log chassisd | match cfeb** command to see error messages that are generated when a Control Board fails or is offline. Use this information to diagnose a Control Board problem and to let JTAC know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Verifying CFEB Failure

Steps To Take To verify CFEB failure, follow these steps:

1. Check the CFEB Uptime on page 426
2. Check the System Uptime on page 427
3. Check the CFEB Connection on page 427
4. Perform a Swap Test on the CFEB on page 427

Step 1: Check the CFEB Uptime

Action To check the CFEB uptime, use the following CLI command:

user@host> **show chassis cfeb**

Sample Output

```
user@host> show chassis cfeb
CFEB status:
Slot 0 information:
  State                              Master
  Intake temperature              29 degrees C / 84 degrees F
  Exhaust temperature             38 degrees C / 100 degrees F
  CPU utilization                  3 percent
  Interrupt utilization            0 percent
  Heap utilization                10 percent
  Buffer utilization              22 percent
  Total CPU DRAM                 128 MB
  Internet Processor II              Version 1, Foundry IBM, Part number 164
  Start time:                        2004-09-28 03:07:54 PDT
  Uptime:                           9 days, 18 hours, 41 minutes, 32 seconds
Slot 1 information:
  State                              Backup
```

What It Means The command output displays how long the CFEB has been operating. A short uptime can indicate a CFEB failure. Look for error messages that were generated at least 5 minutes prior to the failure event by using the following CLI command:

user@host> **show log messages | match cfeb**

Step 2: Check the System Uptime

Action To check the system uptime, use the following CLI command:

user@host> **show system uptime**

Sample Output

```
user@host> show system uptime
Current time:      2002-07-17 16:43:45 PDT
System booted:     2002-07-12 17:29:12 PDT (4d 23:14 ago)
Protocols started: 2002-07-12 17:29:56 PDT (4d 23:13 ago)
Last configured:   2002-07-10 23:10:27 PDT (6d 17:33 ago) by regress
 4:43PM  up 4 days, 23:15, 2 users, load averages: 0.07, 0.02, 0.00
```

What It Means The command output displays the time when the system was last booted, in days and hours. If the boot time is short, it can indicate a Routing Engine or a CFEB failure. Look for error messages that were generated at least 5 minutes prior to the failure event by using the following CLI command:

user@host> **show log messages | match cfeb**

Step 3: Check the CFEB Connection

Action Make sure the CFEB is properly seated in the midplane. Check that the thumbscrews on each CFEB ejector lever are securely tightened. Use a Phillips screwdriver to ensure that the screws are securely tightened.

Step 4: Perform a Swap Test on the CFEB

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the CFEB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

You must power down the CFEB before removing it by pressing and holding down the offline button on the faceplate until the amber LED labeled FAIL lights, or by using the request chassis cfeb offline CLI command.

You must power up the CFEB upon installation by pressing and holding down the offline button on the CFEB faceplate until the green LED labeled Output OK lights steadily, or by using the request chassis cfeb online CLI command.

Action To perform a swap test on a CFEB, follow the procedure in the appropriate routing hardware guide for replacing and installing a CFEB.

Step 5: Perform a Swap Test on the CFEB

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the CFEB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

To perform a swap test on an CFEB, follow the procedure in the *M10i Internet Router Hardware Guide* for replacing and installing a CFEB.

One or two CFEBs can install into the uppermost slots in the rear of the chassis. Only one CFEB is active at a time, with the optional second CFEB in reset mode. CFEBs are hot-pluggable. Removing the standby CFEB has no effect on router function.

If the active CFEB fails or is removed from the chassis, the effect depends on whether two CFEBs are installed:

- If there is only one CFEB, forwarding halts until the CFEB is replaced and functioning again.
- If there are two CFEBs, forwarding halts until the standby CFEB boots and becomes active.

In both cases, all components in the Packet Forwarding Engine reset, and it takes approximately one minute for the new CFEB to become active; synchronizing router configuration information can take additional time, depending on the complexity of the configuration.

Action To perform a swap test on a CFEB, follow these steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis.
3. If you are removing the active CFEB, press and hold the offline button on the faceplate until the amber LED labeled FAIL lights, which takes about 5 seconds. (The effect of removing the active CFEB depends on whether a second CFEB is installed.
4. Loosen the thumbscrew on each ejector lever using a Phillips screwdriver if necessary.
5. Pull the end of each ejector lever outward until it is nearly perpendicular to the CFEB faceplate.
6. Grasp the ejector levers and pull firmly to slide the CFEB about halfway out of the chassis.

7. Place one hand under the CFEB to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

CAUTION: When a CFEB is out of the chassis, do not hold it by the ejector levers. They cannot support the weight of the CFEB.

Do not stack CFEBs on top of or under other components. Place each one individually in an electrostatic bag or on its own antistatic mat on a flat, stable surface.

---

8. Verify that the ends of the ejector levers are pulled outward to a position nearly perpendicular to the faceplate of the CFEB.

9. Place one hand under the CFEB to support it and grasp one of the ejector levers at the front with the other hand.

10. Align the rear of the CFEB with the guides inside the chassis and slide it in completely.

11. Press the ejector lever at each end of the CFEB inward.

Getting CFEB Hardware Information

Steps To Take To display CFEB hardware information, follow these steps:

1. Display the CFEB Hardware Information on page 429
2. Display the CFEB Firmware Information on page 430
3. Locate the CFEB Serial Number ID Label on page 430

Step 1: Display the CFEB Hardware Information

Action To display the CFEB hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                30512             M7i
Midplane         REV 04   710-008761   CB9213            M7i Midplane
Power Supply 0   Rev 02   740-008985   QB12884           DC Power Supply
Routing Engine   REV 09   740-009459   1000482742        RE-5.0
CFEB             REV 04   750-010112   CB8664            Internet Processor II
FPC 0                                                    E-FPC
FPC 1                                                    E-FPC
  PIC 2                   BUILTIN      BUILTIN           1x Tunnel
  PIC 3          REV 04   750-009099   CB9103            1x G/E, 1000 BASE
```

What It Means The command output displays the CFEB version level, part number, serial number, and description.

Step 2: Display the CFEB Firmware Information

Action To display the firmware running on the CFEB, use the following CLI command:

user@host> **show chassis firmware**

Sample Output

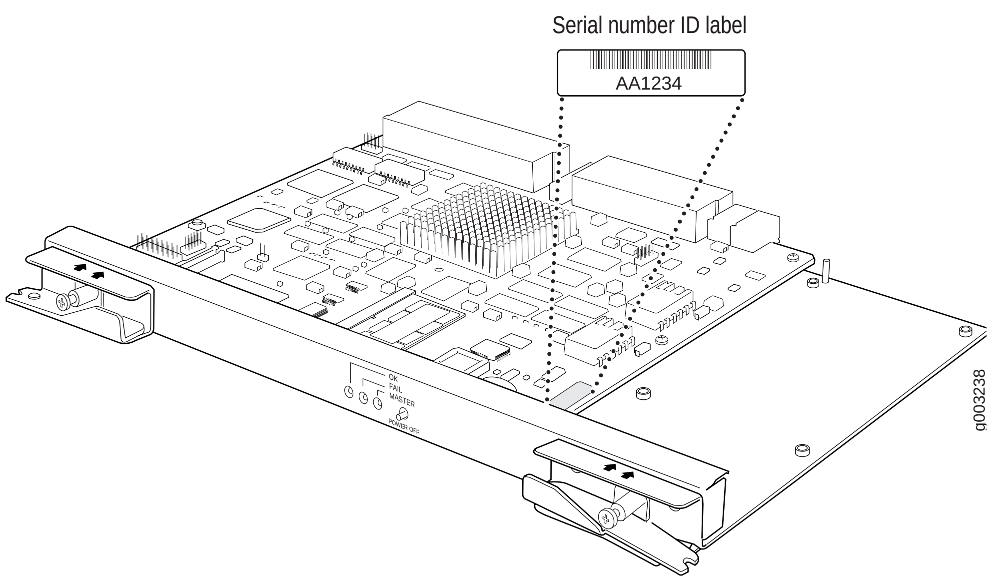
```
user@host> show chassis firmware
Part                     Type       Version
[...Output truncated...]
CFEB                     ROM        Juniper ROM Monitor Version 6.0b12
                         O/S        Version 7.0I14 by bharani on 2004-09-14 17:
```

What It Means The command output displays the type and version level of the firmware running on the CFEB.

Step 3: Locate the CFEB Serial Number ID Label

Action To locate the CFEB serial number ID label, look on the right side of the top panel (see Figure 172).

Figure 172: CFEB Serial Number ID Label



Returning the CFEB

Action To return the CFEB, see "Return the Failed Component" on page 86 or follow the procedure in the appropriate router hardware guide.

Chapter 33

Monitoring the HCM

You monitor the High-Availability Chassis Manager (HCM) on the M10i router to ensure that it works with its companion Routing Engine to provide control and monitoring functions for router components. You also monitor the HCM to ensure that it displays alarm status and takes Physical Interface Cards (PICs) online and offline. (See Table 100.)

Table 100: Checklist for Monitoring the HCM

Monitor HCM Tasks	Command or Action
Understanding the HCM on page 433	
Monitoring the HCM Status on page 434	
1. Check HCM LEDs on page 435	Look at the LEDs on the HCM component faceplate.
2. Check HCM Environmental Status on page 435	show chassis environment hcm
3. Check the Companion Routing Engine Status on page 435	show chassis routing-engine
Displaying HCM Alarms on page 437	show chassis alarms
Performing A Swap Test on page 438	
1. Remove An HCM on page 438	Remove the HCM and replace it with one that you know works. Follow the procedure in the *M10i Internet Router Hardware Guide* to remove an HCM. 1. If two HCMs are installed, determine which HCM is master using the show chassis environment hcm CLI command. 2. Switch HCM mastership using the request chassis routing-engine master switch CLI command. 3. Shut down the router software using the request system halt CLI command. 4. Remove the Routing Engine. 5. Remove the failed HCM.
6. Install an HCM on page 440	1. Install the HCM that works. 2. Install the Routing Engine. 3. Ensure that the HCM is functioning properly using the show chassis environment hcm CLI command. If the HCM still doesn't work, return it. See "Return the Failed Component" on page 86 or follow the procedure described in the *M10i Internet Router Hardware Guide*.

Monitor HCM Tasks	Command or Action
Getting HCM Hardware Information on page 441	
1. Display the HCM Hardware Information on page 441	show chassis hardware
2. Locate the HCM Serial Number ID Label on page 442	Look near the front of the component on the right side.
Returning the HCM on page 442	See "Return the Failed Component" on page 86, or follow the procedure in the *M10i Internet Router Hardware Guide*.

Understanding the HCM

Purpose Inspect the HCM to ensure that it works with its companion Routing Engine to provide control and monitoring functions for routing components. Also, inspect the HCM to ensure that it displays alarm status and takes the PIC online and offline.

What Is an HCM The HCM on the M10i router performs the following functions:

- Monitoring and control of router components—The HCM collects statistics from all sensors in the system. When it detects a failure or alarm condition, it sends a signal to the Routing Engine, which generates control messages or sets an alarm. The HCM also relays control messages from the Routing Engine to the router components.

- Controlling component power-up and power-down—The HCM controls the power-up sequence of router components as they start and powers down components when their offline buttons are pressed.

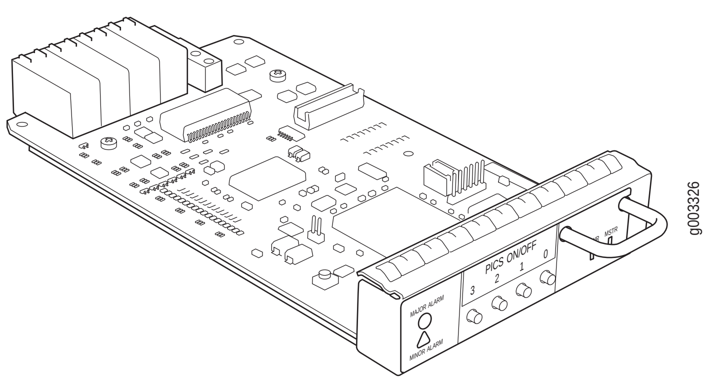
- Signaling of mastership—In a router with more than one Routing Engine, the HCM signals to all router components which Routing Engine is the master and which is the standby.

- Alarm display—The HCM provides status and troubleshooting information at a glance. It is located on the front of the chassis below the FPC card cage, as shown in Figure 174. The LEDs on the HCM include two alarm LEDs. The circular red alarm LED at the upper right of the craft interface indicates a critical condition that can result in a system shutdown. The triangular yellow alarm below it indicates a less severe condition that requires monitoring or maintenance. Both alarms can occur simultaneously.

- PIC removal—If a PIC offline button is pressed, the HCM relays the request to the Compact Forwarding Engine Board (CFEB), which takes the PIC offline and informs the Routing Engine. Other PICs are unaffected, and system operation continues. For more information, see “PIC Offline Buttons” on page 21.

Figure 173 shows the M10i router HCM component.

Figure 173: M10i Router HCM Component

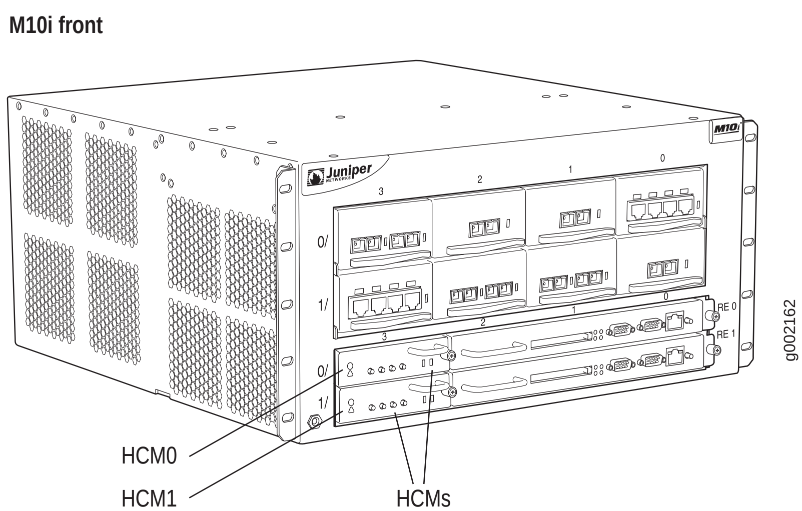


The HCM has the following components:

- 100-Mbps Fast Ethernet switch—Carries signals and monitoring data between router components.
- Two LEDs—Indicate HCM status. The green LED is labeled PWR and the blue LED labeled MSTR. See "HCM LEDs" on page 435 for a description of the LED states.
- Alarm LEDs—Display alarm conditions, if any exist.
- PIC offline buttons—Relay a request to the CFEB, which prepares a PIC for removal from the router, or brings the PIC online when it is replaced.

Two HCMs are installed into the midplane from the front of the chassis, as shown in Figure 174. The master HCM performs all functions and provides PIC removal buttons for the first FPC. The standby HCM provides PIC removal buttons for the second FPC. The HCM in the slot labeled HCM0 is paired with the Routing Engine in the slot labeled RE0. Likewise, the HCM in the slot labeled HCM1 is paired with the Routing Engine in the slot labeled RE1. By default, the HCM in the slot labeled HCM0 is the master.

Figure 174: M10i Router HCM Location



The HCM is hot-pluggable.

Monitoring the HCM Status

Steps To Take To monitor the HCM status, follow these steps:

1. Check HCM LEDs on page 435
2. Check HCM Environmental Status on page 435

3. Check the Companion Routing Engine Status on page 435

Step 1: Check HCM LEDs

Action To check the HCM LEDs, look at the component faceplate at the bottom left front of the M10i router chassis (see Figure 174 on page 434).

Two LEDs indicate HCM status—a green PWR LED and a blue MSTR LED. Table 101 describes the LED states.

Table 101: HCM LEDs

Label	Color	State	Description
PWR	Green	On steadily	HCM is functioning normally.
		Blinking	HCM is starting up.
MSTR	Blue	On steadily	HCM is master.

Step 2: Check HCM Environmental Status

Action To chck the HCM environmental status, use the following CLI command:

user@host: **show chassis environment hcm**

Sample Output

```
user@host> show chassis environment hcm
HCM 0 status:
  State                            Online Master
  FPGA Revision                27
HCM 1 status:
  State                            Present Standby
  FPGA Revision                27
```

What It Means The command output shows that the HCM status, including slot number, operating state, and field programmable gate array (FPGA) revision.

Alternative Action To display the environmental status of a particular HCM, use the following CLI command:

```
m10i@host> show chassis environment hcm slot
```

Step 3: Check the Companion Routing Engine Status

The HCM in the slot labeled HCM0 is paired with the Routing Engine in the slot labeled RE0. Likewise, the HCM in the slot labeled HCM1 is paired with the Routing Engine in the slot labeled RE1. By default, the HCM in the slot labeled HCM0 is the master.

When HCM mastership changes because of failure, Routing Engine mastership changes as well.

Action To check Routing Engine status, use the following CLI command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
```

```
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 36 degrees C / 96 degrees F
    CPU temperature             35 degrees C / 95 degrees F
    DRAM                       256 MB
    Memory utilization          37 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     6 percent
      Interrupt                  0 percent
      Idle                      93 percent
    Model                          RE-5.0
    Serial ID                      1000488824
    Start time                     2004-09-28 03:06:10 PDT
    Uptime                        13 days, 10 hours, 36 minutes, 22 seconds
    Load averages:                 1 minute   5 minute  15 minute
                                       0.22       0.06       0.02
Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 35 degrees C / 95 degrees F
    CPU temperature             32 degrees C / 89 degrees F
    DRAM                       256 MB
    Memory utilization          28 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     1 percent
      Interrupt                  0 percent
      Idle                      99 percent
    Model                          RE-5.0
    Serial ID                      1000485860
    Start time                     2004-09-11 01:01:02 PDT
    Uptime                        30 days, 12 hours, 41 minutes, 15 seconds
```

What It Means The command output displays the operating state of both Routing Engines installed in the router chassis, including slot number, current state, and default election priority—master or backup. The command output also displays the Routing Engine temperature, amount of memory, and the percentage of memory and CPU utilization. The command output displays the Routing Engine model number, serial number ID, start time, and total operating time.

Alternative Action Look at the Routing Engine LEDs by using the show chassis routing-engine CLI command or by looking at the component faceplate at the front of the router. The Routing Engine has four LEDs that tell operating status: agreen LED labeled HDD, a blue LED labeled MASTER, a red LED labeled FAIL, and a green LED labeled ONLINE. Table 102 describes the Routing Engine LED states.

Table 102: Routing Engine LEDs

Label	Color	State	Description
HDD	Green	Blinking	There is read/write activity on the PC card.
MASTER	Blue	On steadily	Routing Engine is functioning as master.

Label	Color	State	Description
FAIL	Red	On steadily	Routing Engine is not operational..
ONLINE	Green	On steadily	Routing Engine is running normally.

Displaying HCM Alarms

If a router with a single HCM fails, no alarm can be sent. If a master HCM fails on a router with dual HCMs and the backup HCM takes over mastership, an alarm is reported on the backup Routing Engine.

When HCM mastership changes because of failure, Routing Engine mastership changes as well.

Action To view HCM alarms, use the following CLI command:

user@host> show chassis alarms

Sample Output

```
user@host> show chassis alarms
4 alarms currently active
Alarm time              Class  Description
2005-02-16 22:10:27 UTC  Minor  Backup RE Active
```

What It Means The command output displays a minor alarm indicating that the backup Routing Engine is active or is master. Since the HCM is a companion component of the Routing Engine, the backup HCM is also active. The command output displays the date and time of the alarm.

To verify that the backup HCM has taken over mastership, use the show chassis routing-engine CLI command.

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Master (default)
    Temperature                 33 degrees C / 91 degrees F
    DRAM                      2048 MB
    Memory utilization          13 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     0 percent
      Interrupt                  0 percent
      Idle                     100 percent
    Model                          RE-3.0
    Serial ID                      P10865703096
    Start time                     2005-02-16 22:13:19 UTC
    Uptime                        2 hours, 13 minutes, 57 seconds
Routing Engine status:
  Slot 1:
    Current state                  Master
    Election priority              Backup (default)
    Temperature                 33 degrees C / 91 degrees F
    CPU temperature             29 degrees C / 84 degrees F
    DRAM                      2048 MB
```

```
Memory utilization          12 percent
CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     3 percent
  Interrupt                  0 percent
  Idle                      97 percent
Model                          RE-3.0
Serial ID                      P10865701255
Start time                     2005-02-03 03:13:39 UTC
Uptime                        13 days, 21 hours, 12 minutes, 35 seconds
Load averages:                 1 minute   5 minute  15 minute
                                   0.00       0.03       0.01
```

What It Means The HCM in the slot labeled HCM0 is paired with the Routing Engine in the slot labeled RE0. Likewise, the HCM in the slot labeled HCM1 is paired with the Routing Engine in the slot labeled RE1. By default, the HCM in the slot labeled HCM0 is the master. However, in this instance, the Routing Engine in slot RE1 has taken over mastership, indicating that the HCM in slot HCM1 is also master.

Performing A Swap Test

NOTE: although steps to remove and install an HCM are provided here, ensure that you refer to the appropriate hardware guide for the latest information.

Before performing a swap test, always check for bent pins in the midplane and check the HCM for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

The HCM is hot-pluggable. You can perform a swap test on an HCM to pinpoint the problem.

Action To perform a swap test and verify HCM failure, follow these steps:

Steps To Take

1. Remove An HCM on page 438
2. Install an HCM on page 440

Step 1: Remove An HCM

The HCM is hot-pluggable. You can perform a swap test on an HCM to try to pinpoint the problem.

Action To remove an HCM, follow these steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface.
2. If a Routing Engine is installed in the same row as the HCM you are removing, remove the Routing Engine first. If two Routing Engines are installed, use one of the following two methods to determine which HCM is functioning as master:
   - Note which of the blue MASTER LEDs is lit on the Routing Engine faceplates.
   - Use the following CLI command:

user@host> **show chassis environment hcm**

```
HCM 0 status:
    State                           Online Master
    FPGA Revision                27
HCM 1 status:
    State                           Online Standby
    FPGA Revision                27
```

The master HCM is designated Master in the State field.

3. If you are removing the master Routing Engine and a second Routing Engine is installed, issue the following CLI command to switch mastership to the standby host module:

   user@host> **request chassis routing-engine master switch**

   ```
   warning: Traffic will be interrupted while the PFE is re-initialized
   Toggle mastership between routing engines ? [yes,no] (no) yes

   Resolving mastership...
   ```

   If the Routing Engines are running JUNOS Release 6.0 or later and are configured for graceful switchover, the standby Routing Engine immediately assumes Routing Engine functions and there is no interruption to packet forwarding. Otherwise, packet forwarding halts while the standby Routing Engine becomes the master and the Packet Forwarding Engine components reset and connect to the new master Routing Engine. For information about configuring graceful switchover, see the section about Routing Engine redundancy in the *JUNOS System Basics Configuration Guide*.

NOTE: Router performance might change if the standby Routing Engine's configuration differs from the former master's configuration. For the most predictable performance, configure the two Routing Engines identically, except for parameters unique to a Routing Engine, such as the hostname defined at the [edit system] hierarchy level and the management interface (fxp0 or equivalent) defined at the [edit interfaces] hierarchy level.

To configure Routing Engine-specific parameters and still use the same configuration on both Routing Engines, include the appropriate configuration statements under the re0 and re1 statements at the [edit groups] hierarchy level and use the apply-groups statement. For instructions, see the *JUNOS System Basics Configuration Guide.*

4. On the console or other management device connected to the Routing Engine, enter CLI operational mode and use the following command to shut down the router software cleanly and preserve Routing Engine state information:

   user@host> **request system halt**

   Wait until a message appears on the console confirming that the operating system has halted.

For more information about the command, see the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

NOTE: The router might continue forwarding traffic for a few minutes after the request system halt command has been issued.

5. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis.

6. Loosen the thumbscrews located at each end of the Routing Engine faceplate, using a Phillips screwdriver if necessary.

7. Grasp the handle and slide the unit about halfway out of the chassis.

CAUTION: Slide the Routing Engine straight out of the chassis. Damage can result if it gets lodged because of uneven movement.

8. Place one hand under the Routing Engine to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

9. Grasp the handle of the HCM and slide the unit about halfway out of the chassis.

CAUTION: Slide the HCM straight out of the chassis. Damage can result if it gets lodged because of uneven movement.

10. Place one hand under the HCM to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

Step 2: Install an HCM

Action To install an HCM, follow these steps:

1. Attach an ESD grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis.

2. Place one hand under the HCM to support it and grasp the handle on the faceplate with the other hand.

3. Align the rear of the HCM with the guide rails inside the chassis and slide it in completely.

CAUTION: Align the HCM carefully with the guide rails and push it in evenly. Damage can result if it gets lodged in the rails because of uneven movement.

4. Place one hand under the Routing Engine to support it and grasp the handle on the faceplate with the other hand.

5. Align the rear of the Routing Engine with the guide rails inside the chassis and slide it in completely.

CAUTION: Align the Routing Engine carefully with the guide rails and push it in evenly. Damage can result if it gets lodged in the rails because of uneven movement.

---

6. Tighten the thumbscrews on the Routing Engine faceplate to secure the Routing Engine.

7. Use the show chassis environment hcm CLI command to verify that the HCM is functioning correctly.

Getting HCM Hardware Information

Steps To Take To obtain HCM hardware information, follow these steps:

1. Display the HCM Hardware Information on page 441

2. Locate the HCM Serial Number ID Label on page 442

Step 1: Display the HCM Hardware Information

Action To display the HCM hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

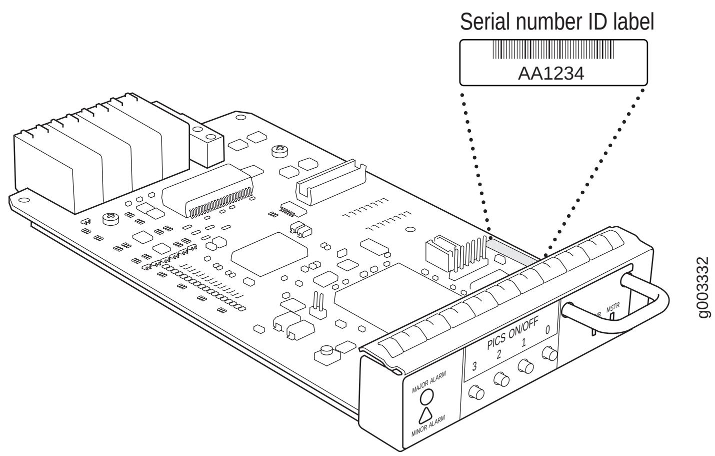
```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                30700             M10i
Midplane         REV 04   710-008920   CB8867            M10i Midplane
Power Supply 0   Rev 05   740-008537   QB12637           AC Power Supply
Power Supply 1   Rev 05   740-008537   QB12537           AC Power Supply
HCM slot 0       REV 05   710-008661   CC1145            M10i HCM
HCM slot 1       REV 05   710-008661   CC1138            M10i HCM
[...Output truncated...]
```

What It Means The command output displays the HCM version level, part number, serial number, and description.

Step 2: Locate the HCM Serial Number ID Label

Action To locate the HCM serial number ID label, look near the front of the component on the right side (see Figure 175).

Figure 175: M10i Router HCM Serial Number ID Label



Returning the HCM

Action To return the HCM, see “Return the Failed Component” on page 86 or follow the instructions in the *M10i Internet Router Hardware Guide*.

Chapter 34

Monitoring the FIC

You monitor the Fixed Interface Card (FIC), which receives incoming packets from the network and transmits outgoing packets to the network, providing support for Fast Ethernet ports or Gigabit Ethernet interfaces, depending on which version of the FIC is installed in the M7i router. You also monitor the FIC to view alarm status, and to perform some system control functions, such as taking Physical Interface Cards (PICs) online and offline. (See Table 103.)

Table 103: Checklist for Monitoring the FIC

Monitor FIC Tasks	Command or Action
Understanding the FIC on page 444	
■ M7i Router FIC with Fast Ethernet Ports on page 444	
■ M7i Router FIC with Gigabit Ethernet Port on page 444	
■ M7i Router FIC Location on page 444	
■ FIC Numbering on page 445	
Monitoring the FIC Status on page 445	
1. Understand FIC Slot Numbering on page 445	The FIC is located in FPC 1 slot 3.
2. Display FIC Status at the Command Line on page 445	show chassis pic pic-slot 3 fpc-slot 1
3. Check FIC LEDs on page 446	Look at the FIC faceplate LEDs.
Displaying FIC Alarms on page 446	
1. Display the FIC Status on page 446	show chassis pic pic-slot 3 fpc-slot 1
2. Display FIC Errors In the nmessages Log File on page 446	show log messages | match PIC 3
3. Display FIC Errors In the chassisd Log File on page 447	show log chassisd | match PIC 3
Verifying FIC Failure on page 447	Look at the FIC faceplate LEDs.
Displaying FIC Hardware Information on page 448	
1. Display the FIC Hardware Information on page 448	show chassis hardware
2. Display the M7i Router Chassis Serial Number on page 448	show chassis hardware
Removing the FIC on page 449	You cannot remove the FIC. It is built into the M7i router chassis.
Returning the FIC on page 449	See "Return the Failed Component" on page 86, or follow the procedure in the *M7i Hardware Guide*.

Understanding the FIC

Purpose Inspect the FIC to ensure that it receives incoming packets from the network, transmits outgoing packets to the network, provides support for Ethernet ports, displays system alarms, and takes PICs online or offline as needed.

What Is an FIC A FIC is a component, built into the M7i router chassis, that receives incoming packets from the network and transmits outgoing packets to the network, providing support for Fast Ethernet ports or Gigabit Ethernet interfaces, depending on which version of the FIC is installed in the M7i router. You also monitor the FIC to view alarm status, and to perform some system control functions, such as taking PICs online and offline.

There are two types of FICs: with fast Ethernet ports and with a Gigabit Ethernet port. Figure 176 shows the FIC with Fast Ethernet ports.

Figure 176: M7i Router FIC with Fast Ethernet Ports

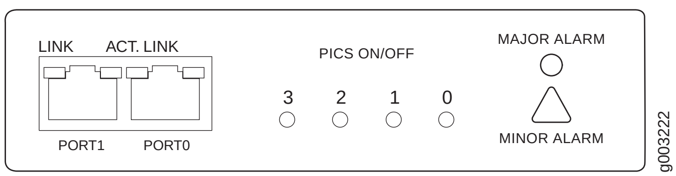
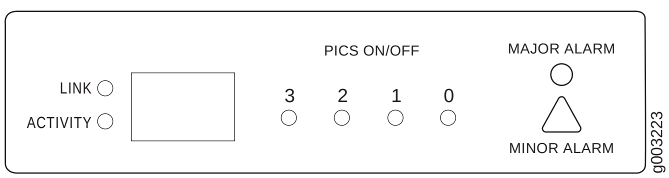


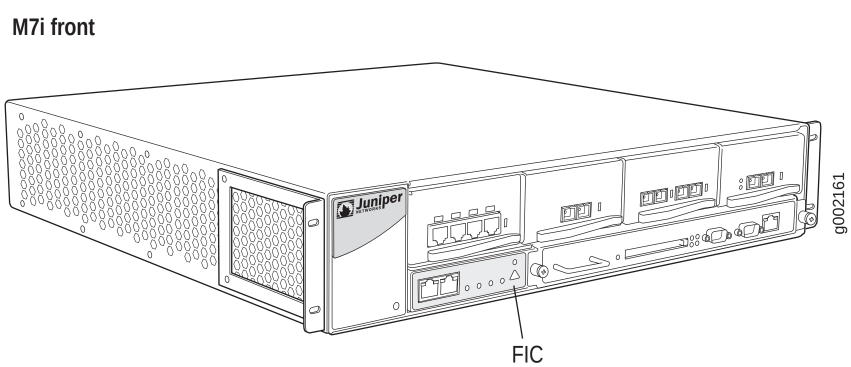
Figure shows the FIC with a Gigabit Ethernet port.

Figure 177: M7i Router FIC with Gigabit Ethernet Port



The FIC is located on the front of the chassis to the left of the Routing Engine and is not a field-replaceable unit (FRU) (see Figure 178).

Figure 178: M7i Router FIC Location



Monitoring the FIC Status

If the FIC fails, no information about chassis components is available through the JUNOS software command-line interface (CLI).

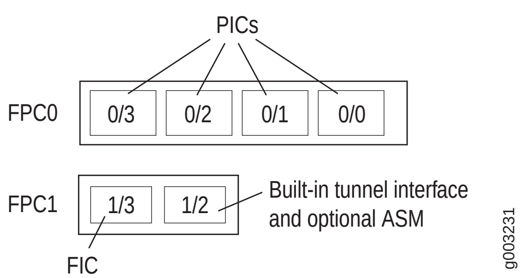
Steps To Take To monitor the FIC status, follow these steps:

1. Understand FIC Slot Numbering on page 445
2. Display FIC Status at the Command Line on page 445
3. Check FIC LEDs on page 446

Step 1: Understand FIC Slot Numbering

Figure 179 shows the FIC location and numbering in the M7i router. The FIC is located in FPC 1 slot 3.

Figure 179: FIC Numbering



Step 2: Display FIC Status at the Command Line

Action To display the FIC status, use the following CLI command:

user@host> **show chassis pic pic-slot 3 fpc-slot 1**

Sample Output

```
user@host> show chassis pic pic-slot 3 fpc-slot 1
PIC fpc slot 1 pic slot 3 information:
  Type                             1x G/E, 1000 BASE
  ASIC type                        QGE FPGA
  State                            Online
  PIC version                  1.4
  Uptime                        12 hours, 11 minutes, 39 seconds

PIC Port Information:
  Port        Cable             SFP                 SFP Vendor
  Number      Type              Vendor Name         Part Number
  0           UNKNOWN CABLE
```

What It Means Since the FIC is located in FPC 1 slot 3, you must specify its location with the show chassis pic CLI command. The command output displays the FIC information, such as the FIC type, ASIC type, operating status, PIC version, and the amount of time the FIC has been online. The command output also displays port cable information.

Step 3: Check FIC LEDs

Table 6 describes the FIC interface LEDs located on the FIC faceplate.

Table 104: Table 6: FIC Interface LEDs

Label	Color	State	Description
LINK	Green	On steadily	The port is online.
ACTIVITY	Green	Blinking	The port is receiving data.
		Off	The port might be on, but is not receiving data.

Displaying FIC Alarms

Steps To Take To determine whether the FIC is offline, follow these steps:

1. Display the FIC Status on page 446
2. Display FIC Errors In the nmessages Log File on page 446
3. Display FIC Errors In the chassisd Log File on page 447

Step 1: Display the FIC Status

Action To view the FIC status, use the following CLI command:

user@host> **show chassis pic pic-slot 3 fpc-slot 1**

Sample Output

```
user@host> show chassis pic pic-slot 3 fpc-slot 1
PIC fpc slot 1 pic slot 3 information:
  State                            Offline
```

What It Means The FIC in fpc slot 1 pic slot 3 is offline.

Step 2: Display FIC Errors In the nmessages Log File

Action To display the FIC errors recorded in the messages log file, use the following CLI command:

user@host> **show log messages | match PIC 3**

Sample Output

```
user@host> show log messages | match PIC 3 in FPC 1
Feb 22 05:50:58  noah chassisd[4738]: CHASSISD_PIC_OFFLINE_NOTICE: Taking PIC 3
in FPC 1 offline: Offlined by cli command
Feb 22 05:50:58  noah cfeb CMFPC: Offline CMD request for PIC 1/3
Feb 22 05:50:58  noah chassisd[4738]: CHASSISD_IFDEV_DETACH_PIC:
ifdev_detach_pic(1/3)
Feb 22 05:50:58  noah chassisd[4738]: CHASSISD_SNMP_TRAP9: SNMP trap generated:
FRU power off (jnxFruContentsIndex 8, jnxFruL1Index 2, jnxFruL2Index 4,
jnxFruL3Index 0, jnxFruName PIC: 2x F/E, 100 BASE-TX @ 1/3/*, jnxFruType 11,
jnxFruSlot 2, jnxFruOfflineReason 7, jnxFruLastPowerOff 30713054,
jnxFruLastPowerOn 407915)
```

What It Means The messages log file records the error events during the time the FIC went offline. The messages log file records the time and date and the SNMP trap message generated.

Step 3: Display FIC Errors In the chassisd Log File

Action To display FIC errors in the chassisd log file, follow these steps:

user@host> **show log chassisd | match PIC 3**

Sample Output

```
user@host> show log messages | match PIC 3 in FPC 1
Feb 22 05:57:02 PIC message op 1
Feb 22 06:04:35 CHASSISD_PIC_OFFLINE_NOTICE: Taking PIC 3 in FPC 1 offline:
Offlined by cli command
Feb 22 06:04:35 send: fpc 1 pic 3 offline cmd
Feb 22 06:04:36 pic offline req, pic 3, fpc 1
Feb 22 06:04:36 CHASSISD_IFDEV_DETACH_PIC: ifdev_detach_pic(1/3)
Feb 22 06:04:36 send pic_offline_ack fpc 1 pic 3 accept 1
Feb 22 06:04:36 CHASSISD_SNMP_TRAP9: SNMP trap generated: FRU power off
(jnxFruContentsIndex 8, jnxFruL1Index 2, jnxFruL2Index 4, jnxFruL3Index 0,
jnxFruName PIC: 2x F/E, 100 BASE-TX @ 1/3/*, jnxFruType 11, jnxFruSlot 2,
jnxFruOfflineReason 7, jnxFruLastPowerOff 30794800, jnxFruLastPowerOn 30749381)
Feb 22 06:04:36 PIC message op 2
Feb 22 06:04:36 Time to clean up PIC FPC 1, PIC 3
Feb 22 06:04:36 PIC message op 3
Feb 22 06:04:36 pic_handle_message: PIC fpc 1 pic 3 got deleted
Feb 22 06:04:36 pic detach, pic 3, fpc 1
```

What It Means The chassisd log file records the time and date of FIC errors. n nIt displays the SNMP trap error message generated.

Verifying FIC Failure

Action To check the status of each port on a FIC or PIC, look at the LED located on the faceplate. See "Check FIC LEDs" on page 446 for more information. For information about the meaning of LED states on different PICs, see the *M7i Internet Router PIC Guide*.

Displaying FIC Hardware Information

Steps To Take To display FIC hardware information, do the following:

1. Display the FIC Hardware Information on page 448
2. Display the M7i Router Chassis Serial Number on page 448

Step 1: Display the FIC Hardware Information

Action To display the FIC hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                30512             M7i
Midplane         REV 04   710-008761   CB9213            M7i Midplane
Power Supply 0   Rev 02   740-008985   QB12884           DC Power Supply
Routing Engine   REV 09   740-009459   1000482742        RE-5.0
CFEB             REV 04   750-010112   CB8664            Internet Processor II
FPC 0                                                    E-FPC
FPC 1                                                    E-FPC
  PIC 2                   BUILTIN      BUILTIN           1x Tunnel
  PIC 3          REV 04   750-009099   CB9103            1x G/E, 1000 BASE
```

What It Means The command output displays the hardware revision level, part number, serial number, and description for the FIC located at FPC 1 PIC 3.

Step 2: Display the M7i Router Chassis Serial Number

If the FIC fails, you have to return the M7i router chassis. To return the M7i router, you must provide the midplane serial number.

Action To display the M7i router chassis serial number, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                31898             M7i
Midplane         REV 04   710-008761   CC7798            M7i Midplane
Power Supply 0   Rev 05   740-008537   QE16641           AC Power Supply
Routing Engine   REV 09   740-009459   1000513705        RE-5.0
[...Output truncated...]
```

What It Means The M7i router midplane serial number is CC7798.

Removing the FIC

NOTE: You cannot remove the FIC. It is built into the M7i router chassis.

Returning the FIC

Action The FIC is built into the M7i router. If the FIC fails, return the M7i router chassis. To replace the M7i router, see “Return the Failed Component” on page 86 or follow the procedure for returning the chassis in the *M7i Internet Router Hardware Guide*.

Part 9

Monitoring M5 and M10 Router-Specific Components

Chapter 35

Monitoring the FEB

You monitor the Forwarding Engine Board (FEB) on an M5 and M10 router to ensure that forwarding processes occur, such as route lookups, incoming data packet allocation, outgoing data packet transfer, and exception and control packet transfer. (See Table 105.)

Table 105: Checklist for Monitoring the FEB

Monitor FEB Tasks	Command or Action
Understanding the FEB on page 454	
Monitoring the FEB Status on page 455	
1. Display the FEB Environmental Status on page 455	show chassis environment
2. Display the FEB Detailed Status on page 456	show chassis feb
Verifying FEB Failure on page 456	
1. Check the FEB Uptime on page 457	show chassis feb
2. Check the System Uptime on page 457	show system uptime
3. Check the FEB Connection on page 457	Check that the screws at the top of the FEB are securely tightened.
4. Perform a Swap Test on the FEB on page 458	1. Power down the router. 2. Remove the FEB. 3. Replace the FEB with one that you know works.
Getting FEB Hardware Information on page 459	
1. Display the FEB Hardware Information on page 459	show chassis hardware
2. Display the FEB Firmware Information on page 459	show chassis firmware
3. Locate the FEB Serial Number ID Label on page 460	Look near the back on the right side of the FEB.
Returning the FEB on page 460	See "Return the Failed Component" on page 86, or follow the procedure in the *M5 and M10 Internet Router Hardware Guide.*

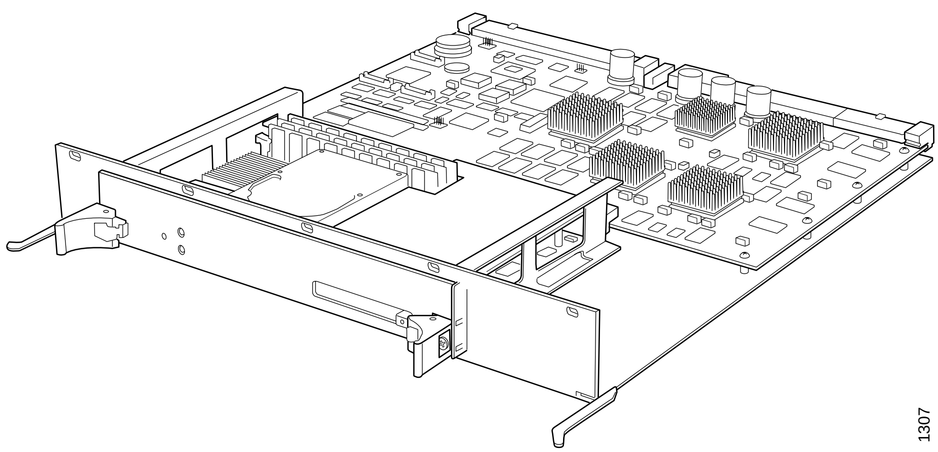
Understanding the FEB

Purpose Inspect the FEB to ensure that communication occurs with the Routing Engine.

What Is an FEB The FEB is a control board for the M5 and M10 routers (see Figure 180). The FEB communicates with the Routing Engine using a dedicated 100-Mbps link that transfers routing table data from the Routing Engine to the forwarding table in the Internet Processor II application-specific integrated circuit (ASIC). The link is also used to transfer routing link-state updates and other packets destined for the router from the FEB to the Routing Engine. The FEB provides the following functions:

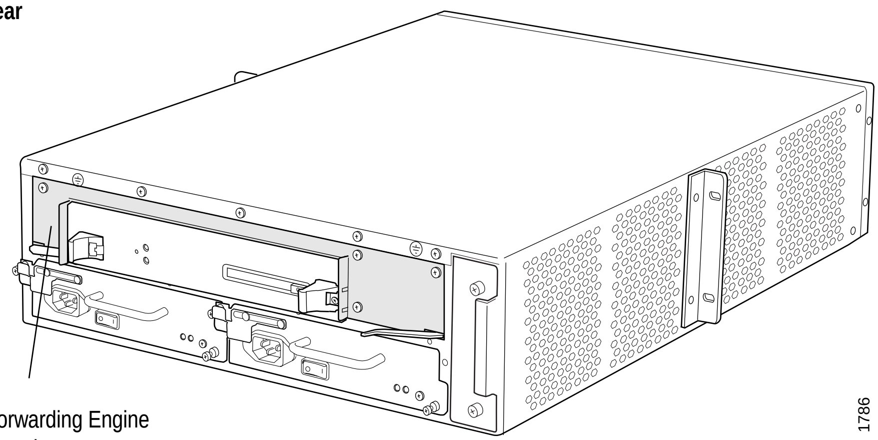
- Route lookups—The Internet Processor II ASIC on the FEB performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM).
- Shared memory management—One Distributed Buffer Manager ASIC on the FEB uniformly allocates incoming data packets throughout the router's shared memory.
- Outgoing data packet transfer—A second Distributed Buffer Manager ASIC on the FEB passes data packets to the destination Physical Interface Card (PIC) when the data is ready to be transmitted.
- Exception and control packet transfer—The Internet Processor II ASIC passes exception packets to the microprocessor on the FEB, which processes almost all of them. The remaining packets are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the FEB are sent to the Routing Engine using system log messages.

Figure 180: FEB Component



The FEB is located on the rear of the router above the power supplies (see Figure 181).

Figure 181: M5 and M10 Router FEB Location



The FEB is field-replaceable, but is not hot-removable or hot-pluggable. You must power down the router before removing or replacing the FEB.

Monitoring the FEB Status

If the FEB fails, no information about chassis components is available through the JUNOS software command-line interface (CLI).

Steps To Take To monitor the FEB status, follow these steps:

1. Display the FEB Environmental Status on page 455
2. Display the FEB Detailed Status on page 456

Step 1: Display the FEB Environmental Status

Action To display the FEB environmental status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@m5-host> show chassis environment
Class Item                   Status     Measurement

Power Power Supply A         OK
      Power Supply B         OK

Temp  FPC Slot 0             OK         32 degrees C / 89 degrees F
      FEB                    OK         31 degrees C / 87 degrees F
      PS Intake              OK         26 degrees C / 78 degrees F
      PS Exhaust             OK         31 degrees C / 87 degrees F
[...Output truncated...]
```

What It Means The command output displays the temperature and status of the FEB, which can be OK, Failed, or Absent.

Step 2: Display the FEB Detailed Status

Action To display more detailed FEB status, use the following CLI command:

user@host> **show chassis feb**

Sample Output

```
user@host> show chassis feb
FEB status:
  Temperature                 37 Centigrade
  CPU utilization              0 percent
  Interrupt utilization        0 percent
  Heap utilization            16 percent
  Buffer utilization          43 percent
  DRAM                        64 Mbytes
  Internet Processor II          Version 1, Foundry IBM, Part number 9
  Start time                     1999-01-24 16:24:42 UTC
  Uptime                         2 hours, 21 minutes, 28 seconds
```

What It Means The command output displays the temperature of the air passing by the FEB, in degrees Centigrade. It displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the FEB processor, including the total DRAM available to the FEB processor. The command output displays the time when the FEB started running and how long the FEB has been running. A short uptime can indicate that there is an FEB problem.

Verifying FEB Failure

The FEB will either restart, keep crashing, or fail completely. If the FEB fails, you will loose the router interface connections.

Steps To Take To verify FEB failure, follow these steps:

1. Check the FEB Uptime on page 457
2. Check the System Uptime on page 457
3. Check the FEB Connection on page 457
4. Perform a Swap Test on the FEB on page 458

Step 1: Check the FEB Uptime

Action To check the FEB uptime, use the following CLI command:

user@host> **show chassis feb**

Sample Output

```
user@host> show chassis feb
FEB status:
  Temperature                24 degrees C / 75 degrees F
  CPU utilization             1 percent
  Interrupt utilization       0 percent
  Heap utilization           17 percent
  Buffer utilization         44 percent
  Total CPU DRAM             64 MB
  Internet Processor II         Version 1, Foundry IBM, Part number 9
  Start time:                   2002-07-12 17:30:43 PDT
  Uptime:                       0 days, 0 hours, 1 minutes, 0 seconds
```

What It Means The command output displays how long the FEB has been operating. A short uptime can indicate an FEB failure. Look for error messages that were generated at least 5 minutes prior to the failure event by using the following CLI command:

user@host> **show log messages**

Step 2: Check the System Uptime

Action To check the system uptime, use the following CLI command:

user@host> **show system uptime**

Sample Output

```
user@host> show system uptime
Current time:      2002-07-17 16:43:45 PDT
System booted:     2002-07-12 17:29:12 PDT (4d 23:14 ago)
Protocols started: 2002-07-12 17:29:56 PDT (4d 23:13 ago)
Last configured:   2002-07-10 23:10:27 PDT (6d 17:33 ago) by regress
 4:43PM  up 4 days, 23:15, 2 users, load averages: 0.07, 0.02, 0.00
```

What It Means The command output displays the time when the system was last booted, in days and hours. If the boot time is short, it can indicate a Routing Engine or an FEB failure. Look for error messages that were generated at least 5 minutes prior to the failure event by using the following CLI command:

user@host> **show log messages**

Step 3: Check the FEB Connection

Action Make sure the FEB is properly seated in the midplane. Use a Phillips screwdriver to ensure that the screws at the top of the FEB are securely tightened.

Step 4: Perform a Swap Test on the FEB

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the FEB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

You must power down the router to remove and replace the FEB.

Action To perform a swap test on an FEB, follow these steps:

1. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.

2. Turn off power to the router. For information on powering down the router, see the *M5 and M10 Internet Router Hardware Guide*.

3. Unscrew the five screws holding the rear chassis component cover in place, and remove the cover. Be sure to save the screws for when you reinstall the cover.

4. Flip the ends of the two ejector levers towards the outside edges of the router.

5. Grasp both sides of the FEB and slide it about three-quarters of the way out of the router.

6. Move one hand underneath the FEB to support it and slide it completely out of the chassis.

7. Remove the Routing Engine from the FEB.

   Unscrew the screws on the outside edges of the extractor clips to unseat the Routing Engine from the FEB. Press in on the red tabs on the extractor clips, then flip the ends of the extractor clips toward the outside edges of the router to release the Routing Engine. Grasp both sides of the Routing Engine and slide it evenly out of the FEB.

8. Replace the Routing Engine in the FEB.

   Align the rear of the unit with the guides inside the chassis. Slide the Routing Engine all the way in until it contacts the connectors on the FEB. Flip the ends of the extractor clips toward the center of the router to seat the Routing Engine onto the FEB. Using a screwdriver, tighten the screws on the outside edges of the extractor clips. Slide the Routing Engine into the slot evenly.

9. Use both hands to grasp the front of the replacement FEB that works and align the rear of the FEB with the guides on the chassis.

10. To ensure proper seating of the ejector levers, move them to an outward position slightly less than perpendicular to the faceplate before seating the FEB in the slot.

11. Slide the FEB all the way into the chassis until it contacts the midplane.

12. Grasp the ejector levers and carefully push the FEB to seat it onto the midplane.

13. Flip the ejector levers toward each other to lodge the FEB in place.

Getting FEB Hardware Information

Steps To Take To obtain FEB hardware information, follow these steps:

1. Display the FEB Hardware Information on page 459
2. Display the FEB Firmware Information on page 459
3. Locate the FEB Serial Number ID Label on page 460

Step 1: Display the FEB Hardware Information

Action To display the FEB hardware information, use the following CLI command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                50974             M10
Midplane         REV 03   710-001950   HA9949
Power Supply A   Rev 03   740-002498   LK33316           DC
Display          REV 04   710-001995   HB2079
Routing Engine                         a000000792cd0a01  RE-2.0
FEB              REV 11   710-001948   HE6497            Internet Processor II
[...Output truncated...]
```

What It Means The command output displays the FEB version level, part number, serial number, and description.

Step 2: Display the FEB Firmware Information

Action To display the firmware running on the FEB, use the following CLI command:

user@host> **show chassis firmware**

Sample Output

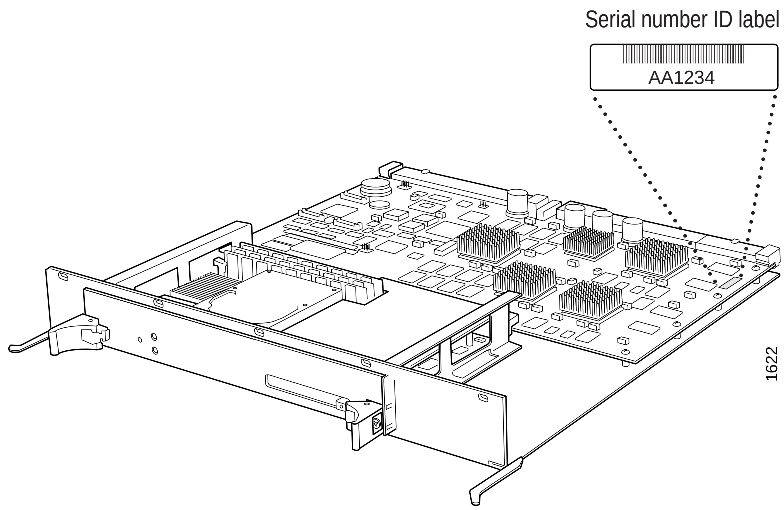
```
user@host> show chassis firmware
Part                     Type       Version
Forwarding engine board  ROM        Juniper ROM Monitor Version 4.1b2
                         O/S        Version 4.1I1 by tlim on 2000-04-24 11:27
```

What It Means The command output displays the type and version level of the firmware running on the FEB.

Step 3: Locate the FEB Serial Number ID Label

Action To locate the FEB serial number ID label, look near the back on the right side of the FEB (see Figure 182).

Figure 182: FEB Serial Number ID Label



Returning the FEB

Action To replace the FEB, see "Return the Failed Component" on page 86 or the *M5 and M10 Internet Router Hardware Guide.*

Part 10

Monitoring Redundant Router Components

Chapter 36

Host Redundancy Overview

You monitor redundant Routing Engines, host modules, and host subsystems to provide a standby Routing Engine and controller component that will switch from standby to active, assuming mastership, with limited running downtime when a failure occurs.

This chapter provides an overview of how redundant host modules, host subsystems, and Routing Engines work on various routing platforms. Additionally, it describes the topics as listed in Table 106.

Table 106: Checklist for Host Redundancy

Monitor Redundant Routing Engine Tasks	Command or Action
Understanding Redundancy for the Routing Engine, Host Module, and Host Subsystem on page 465	
■ M10i Router Redundant Routing Engines and HCMs on page 465 ■ M20 Router Redundant Routing Engines and SSBs on page 466 ■ M40e and M160 Router Redundant Host Modules on page 467 ■ M320 Router, T320 Router, and T640 Routing Node Redundant Host Subsystems on page 468	
Routing Engine, Host Module, and Host Subsystem Redundancy Connections on page 469	
■ Redundancy Connection for an M10i Router on page 470 ■ Redundancy Connection for an M20 Router on page 471 ■ Redundancy Connection for an M40e or M160 Router on page 472 ■ Redundancy Connection for an M320 Router on page 473 ■ Redundancy Connection for a T320 Router and T640 Routing Node on page 474	
Determining Which Routing Engine You Are Logged In To on page 475	
1. Display Routing Engine Status on page 476	show chassis routing-engine
2. Display the Router Hardware on page 476	show chassis hardware
Determining Routing Engine Mastership on page 477	
1. Determine the Routing Engine Mastership By Checking Status on page 477	show chassis routing-engine
2. Determine Routing Engine Mastership By Checking the LEDs on page 478	Physically check the LEDs on either the craft interface or the Routing Engine (depending on which chassis the Routing Engine is installed).
3. Log In To Backup Routing Engine If graceful-switchover is Configured on page 478	request routing-engine login other-routing-engine

Monitor Redundant Routing Engine Tasks	Command or Action
Manually Configuring Master and Backup Routing Engines on page 478	For slot 0: [edit] set chassis redundancy routing-engine 1 master commit For slot 1: [edit] set chassis redundancy routing-engine 0 backup commit
Manually Switching Routing Engine Mastership on page 481	request chassis routing-engine master (acquire | release | switch)
Determining Why Mastership Switched on page 482	show log mastership
Configuring the Backup Routing Engine to Assume Mastership on Failure of Keepalives on page 485	[edit] set chassis redundancy failover on-loss-of-keepalives set chassis redundancy keepalive-time 300 commit
Avoiding Redundancy Problems on page 486	
1. Operate the Same Type of Routing Engine and JUNOS Software on page 486	The active and standby Routing Engines must be the same type of Routing Engine and must operate the same version of JUNOS software.
2. Use the Groups Configuration on page 486	[edit] set groups *group-name*
3. Synchronize Configurations on page 488	[edit] commit synchronize
4. Copy a Configuration File from One Routing Engine to Another on page 488	file copy *<source>* *<destination>*
5. Use the Proper Shutdown Process on a Backup Routing Engine on page 489	request system halt

See Also

- Monitoring Redundant MCSs on page 567
- Monitoring Redundant Routing Engines on page 491
- Monitoring Redundant Control Boards on page 559

Understanding Redundancy for the Routing Engine, Host Module, and Host Subsystem

Purpose

To learn how redundant Routing Engines, host modules, and host subsystems work on various routing platforms. You monitor these components to provide a standby Routing Engine and controller component that will switch from standby to active, assuming mastership when a failure brings down the active master Routing Engine.

What Is a Routing Engine, Host Module, and Host Subsystem Redundancy

Redundant Routing Engines are two Routing Engines that are installed in the same routing platform. One functions as the master, while the other stands by as a backup should the master Routing Engine fail. (See “M10i Router Redundant Routing Engines and HCMs” on page 465 and “M20 Router Redundant Routing Engines and SSBs” on page 466.)

Redundant host modules are two Routing Engine and Miscellaneous Control Subsystem (MCS) pairs installed in the same routing platform. One pair functions as master, while the other stands by as a backup should the master Routing Engine fail. (See “M40e and M160 Router Redundant Host Modules” on page 467.)

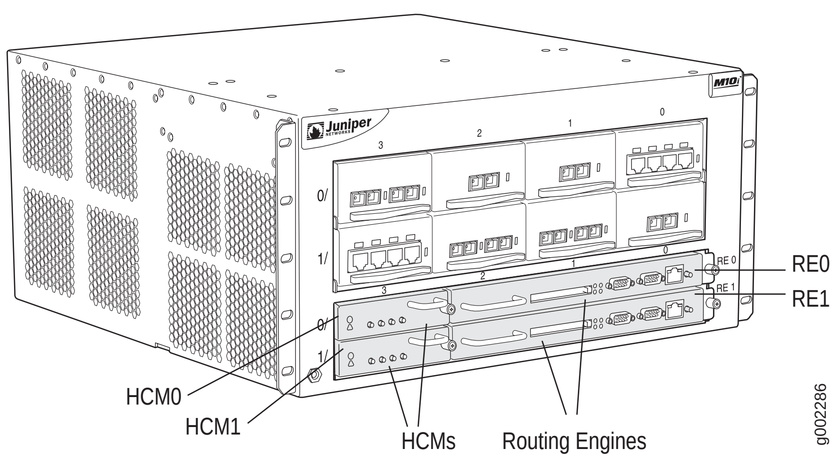
Redundant host subsystems are two Routing Engine and Control Board pairs installed in the same routing platform. One pair functions as master, while the other stands by as backup should the master Routing Engine fail. (See “M320 Router, T320 Router, and T640 Routing Node Redundant Host Subsystems” on page 468.)

The M5, M10, M7i, and M40 routers do not support Routing Engine, host module, or host subsystem redundancy.

M10i Router Redundant Routing Engines and HCMs

On the M10i router, the High-Availability Chassis Manager (HCM) works with its companion Routing Engine to provide control and monitoring functions for router components. The router can have one or two HCMs and Routing Engines. (See Figure 183 and “Redundancy Connection for an M10i Router” on page 470.)

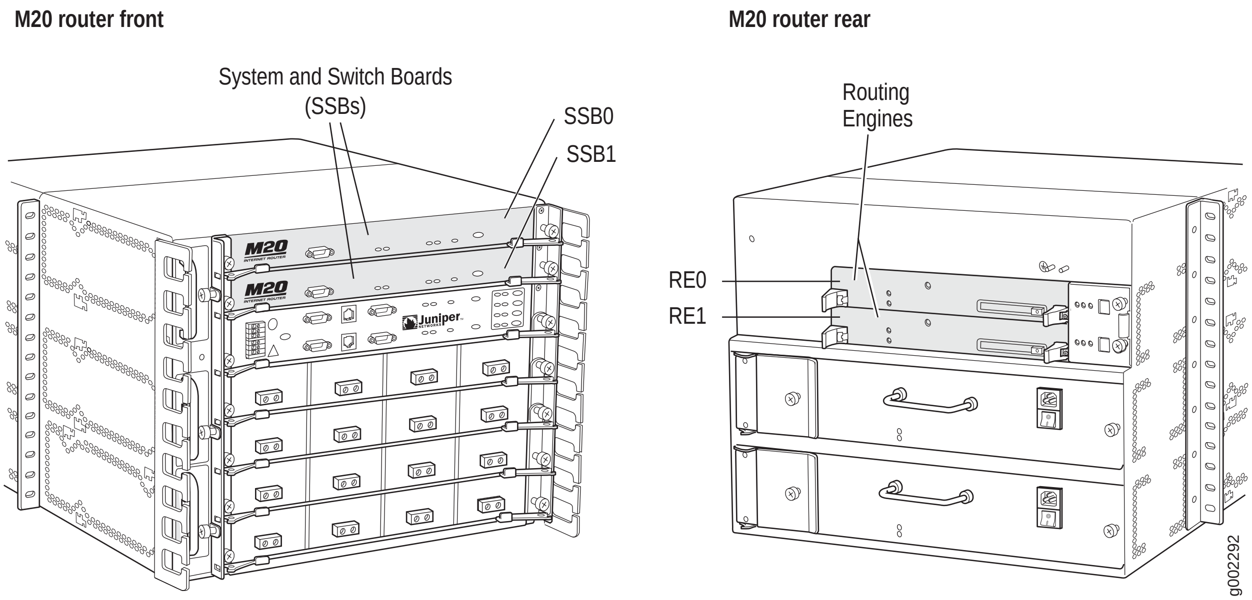
Figure 183: M10i Router Redundant Routing Engines and HCMs



M20 Router Redundant Routing Engines and SSBs

The M20 router can have one or two Routing Engines. The System and Switch Boards (SSBs) communicate with the Routing Engines. (See Figure 184 and "Redundancy Connection for an M20 Router" on page 471.)

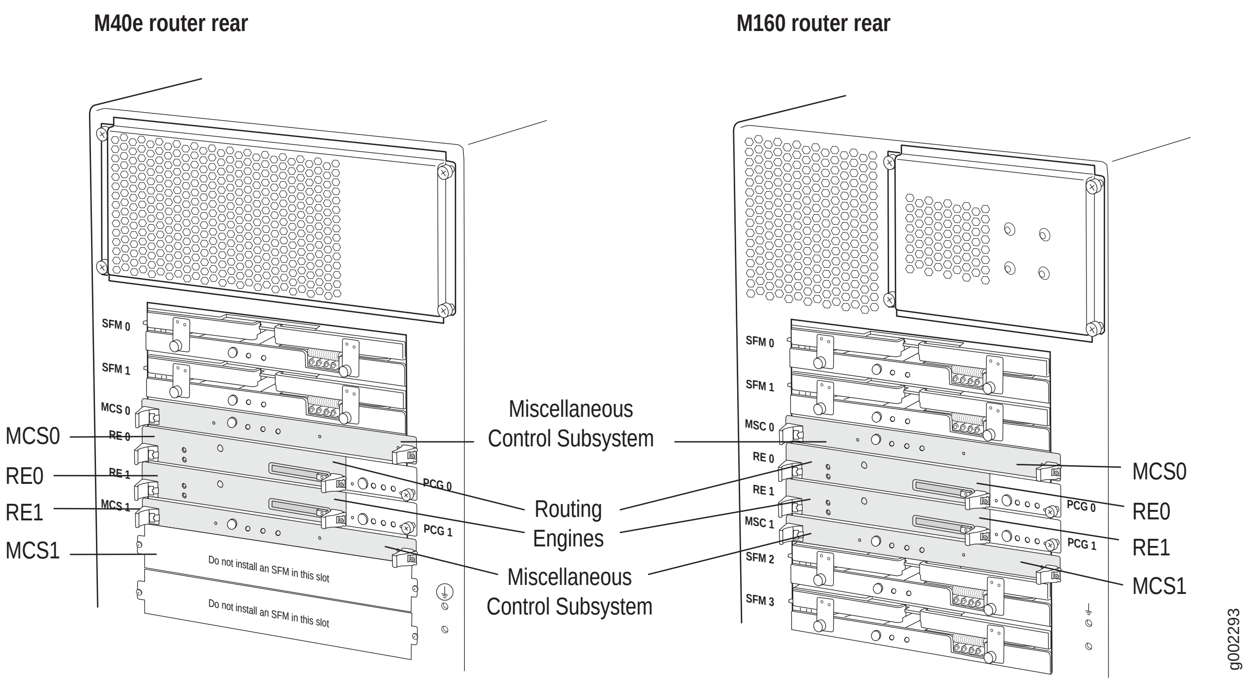
Figure 184: M20 Router Redundant Routing Engines and SSBs



M40e and M160 Router Redundant Host Modules

On M40e and M160 routers, the host module consists of a paired Routing Engine and MCS. One pair functions as master, while the other stands by as a backup should the master Routing Engine fail. (See Figure 185 and “Redundancy Connection for an M40e or M160 Router” on page 472.)

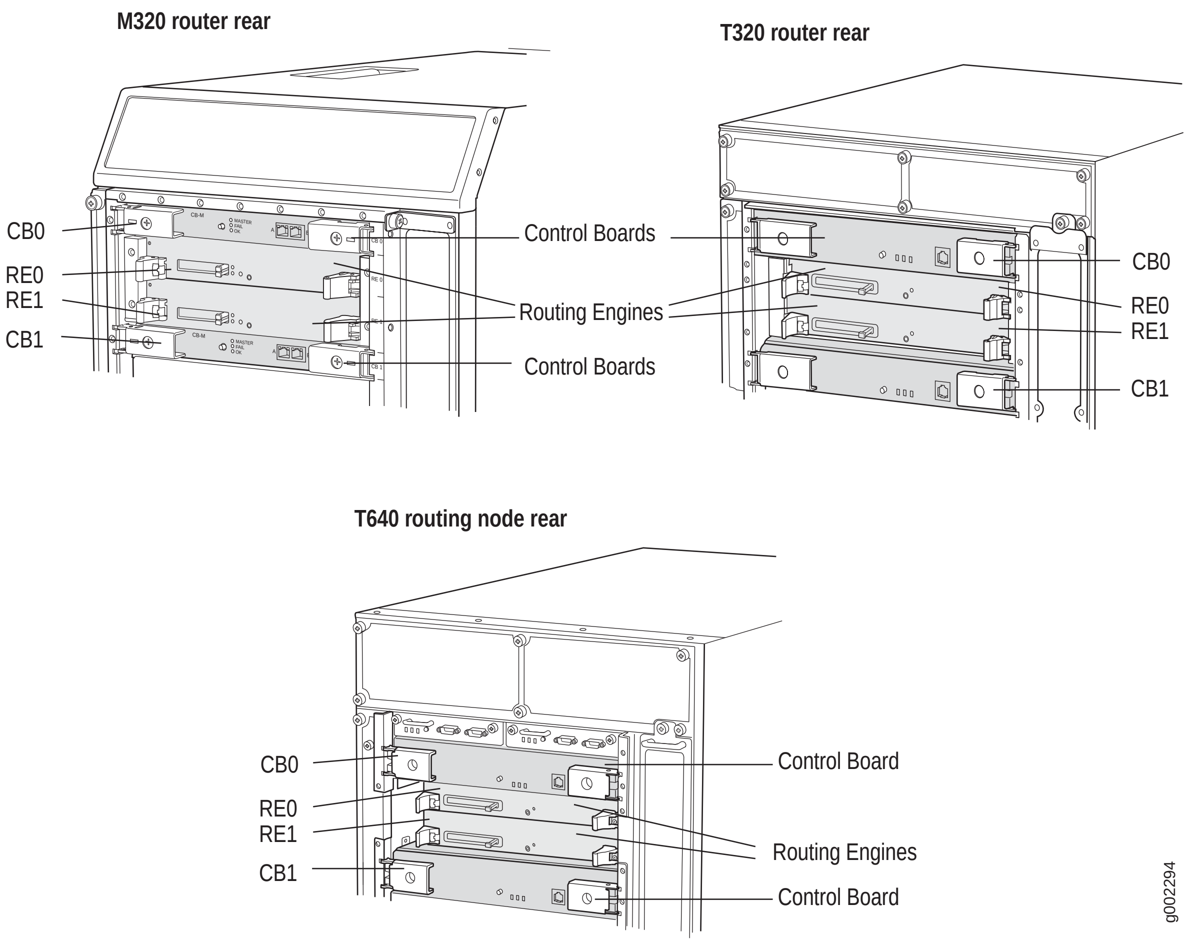
Figure 185: M40e and M160 Router Redundant Host Modules



M320 Router, T320 Router, and T640 Routing Node Redundant Host Subsystems

On the M320 router, T320 router, and the T640 routing node, the host subsystem consists of a Routing Engine and Control Board functioning as a unit. Two host subsystems can be installed in each routing platform. One pair functions as master, while the other stands by as backup should the master Routing Engine fail. (See Figure 186, “Redundancy Connection for an M320 Router” on page 473, and “Redundancy Connection for a T320 Router and T640 Routing Node” on page 474.)

Figure 186: M320 Router, T320 Router, and T640 Routing Node Redundant Host Subsystems



Routing Engine, Host Module, and Host Subsystem Redundancy Connections

It is important to understand how a redundant Routing Engine, redundant host module, or redundant subsystem communicates with its active counterparts to avoid severing the connection used for communication. Severing the connection can potentially trigger a failover protection.

For example, the M160 router active host module (the Routing Engine and the MCS) has the running configuration on it and communicates with the MCS, which in turn communicates with the Flexible PIC Concentrator (FPC) and the Switching and Forwarding Modules (SFMs). The host modules send keepalive messages to each other, checking the operating state. Each host module issues keepalive responses, letting the other host module know that it is up and operating. If keepalive responses are not returned to the standby host module (response times will vary depending upon the time settings specified in the set chassis redundancy keepalive-time statement), the standby host module can become the active host module. (See "Redundancy Connection for an M40e or M160 Router" on page 472.)

You also can configure failover on the router to switch mastership if a critical process fails. If a critical process on the active host module terminates, the standby host module routing becomes the active host module. You can configure processes for which this should happen. For example, you can use the set interface-control failover other-routing-engine statement at the [edit system processes] hierarchy level to configure failover for the interface control daemon.

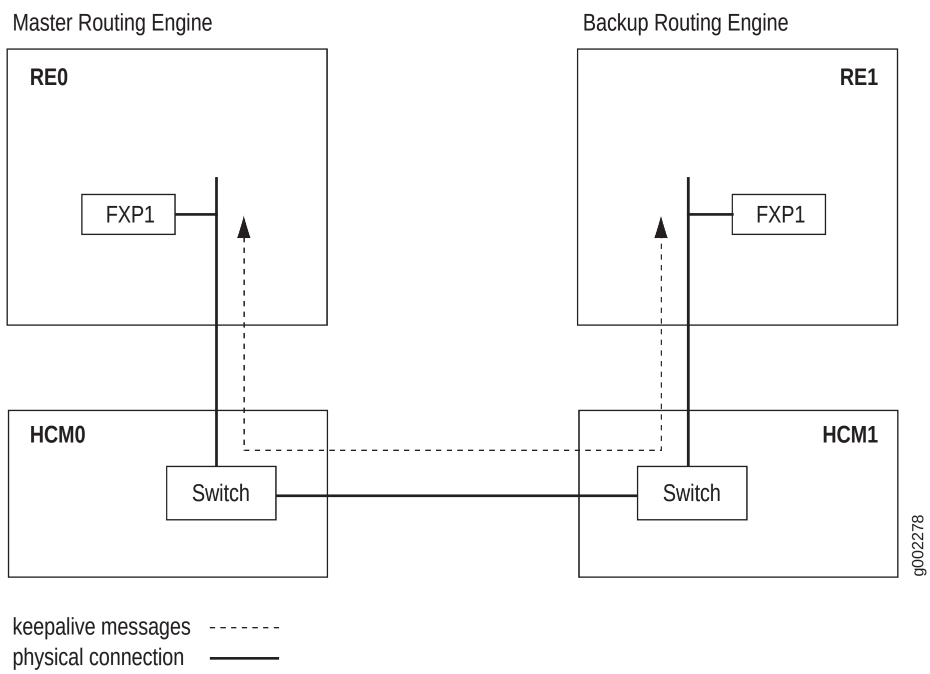
For information about setting keepalive parameters, see "Configuring the Backup Routing Engine to Assume Mastership on Failure of Keepalives" on page 485.

This section includes the following information:

Redundancy Connection for an M10i Router

Figure 187 shows the connection between the master and backup Routing Engines on an M10i router. Keepalive messages are sent between Routing Engines via the interconnected HCM switches. In this way, the master and the backup Routing Engines exchange state information.

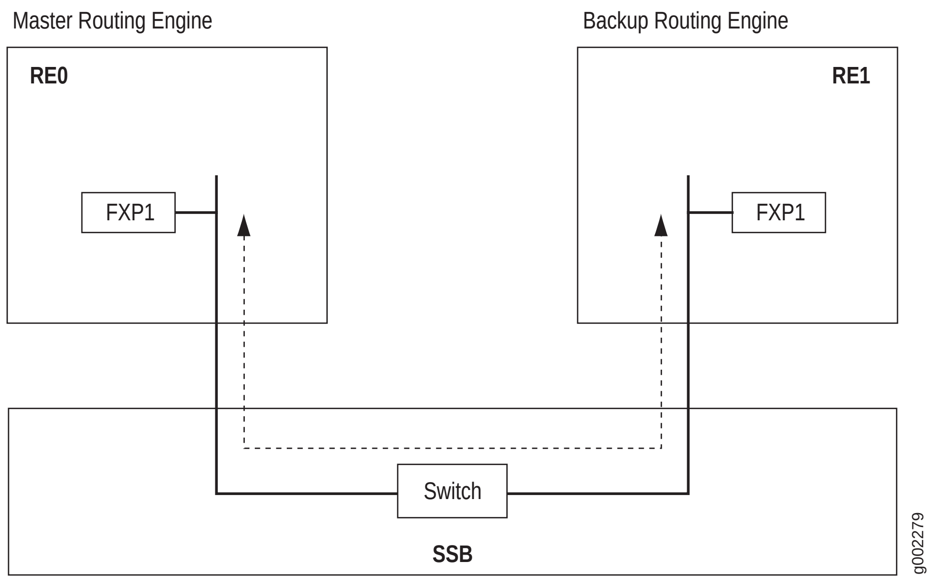
Figure 187: Redundancy Connection for an M10i Router



Redundancy Connection for an M20 Router

Figure 188 shows the connection between the master and backup Routing Engines on an M20 router. Keepalive messages are sent between the master and backup Routing Engine through the switch on the SSB. In this way, the master and the backup Routing Engines exchange state information.

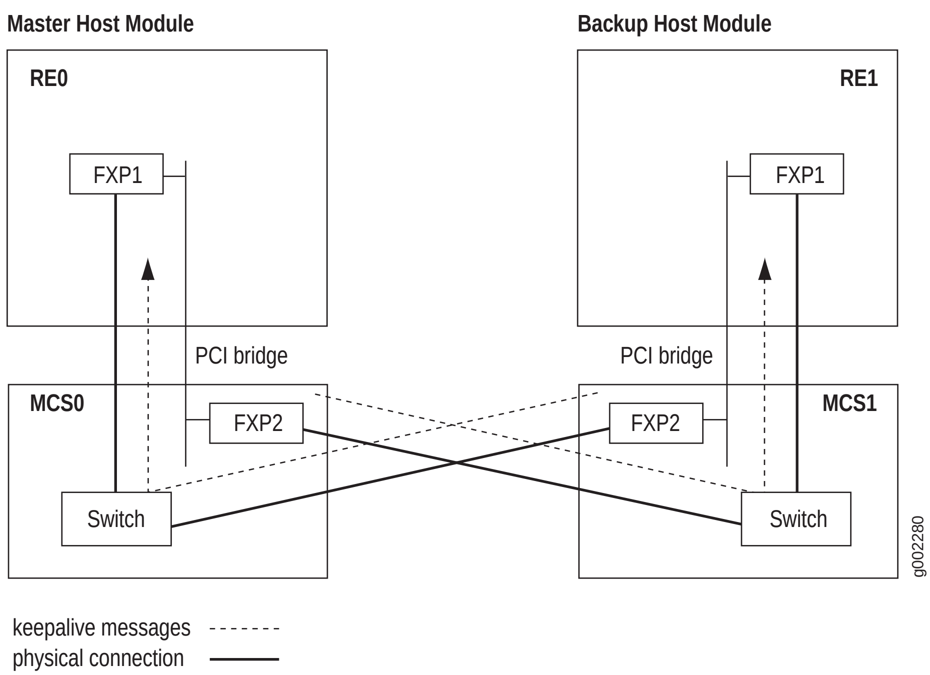
Figure 188: Redundancy Connection for an M20 Router



Redundancy Connection for an M40e or M160 Router

Figure 189 shows the connection between the master and backup host modules on an M40e or M160 router. Keepalive messages are sent from one Routing Engine to the other over the fpx2 interface found across the Peripheral Component Interconnect (PCI) bridge. The keepalive message is received by the other host module via the fpx1 interface. A keepalive response is sent back over the fpx2 interface to the other Routing Engine. In this way, the master and the backup host modules exchange state information.

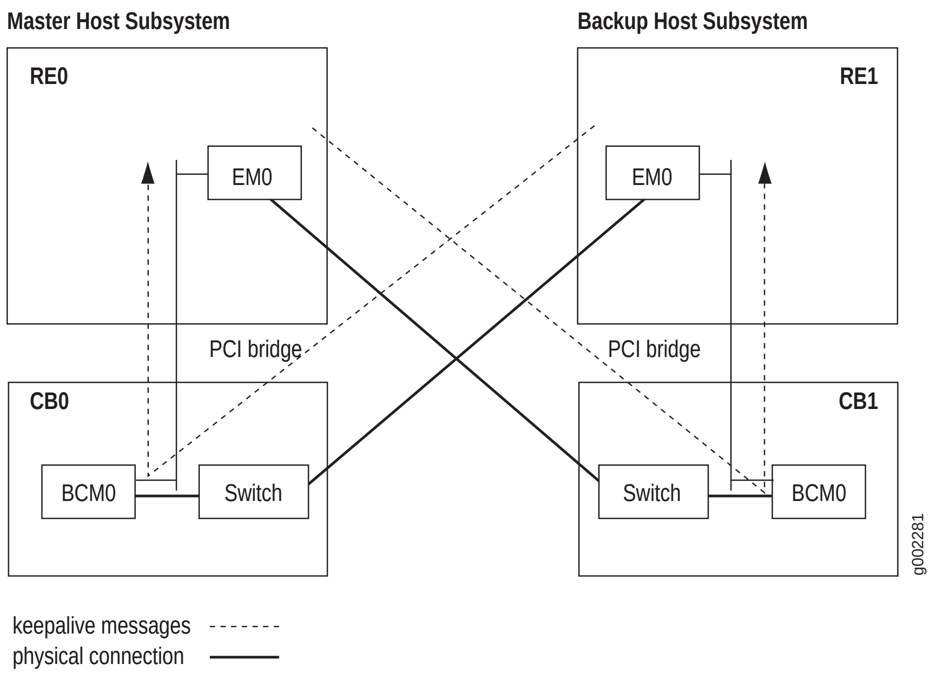
Figure 189: Redundancy Connection for an M40e or M160 Router



Redundancy Connection for an M320 Router

Figure 190 shows the connection between the master and backup host subsystems on an M320 router. Keepalive messages are sent from the Routing Engine over the em0 interface. The keepalive message is forwarded to the other host subsystem via the bcm0 interface on the Control Board. A keepalive response is sent back over the em0 interface to the other Routing Engine. In this way, the master and the backup host subsystems exchange state information.

Figure 190: Redundancy Connection for an M320 Router



Redundancy Connection for a T320 Router and T640 Routing Node

Figure 191 shows the connection between the master and backup host modules on a T320 router or a T640 routing node with a Routing Engine 600 (RE-600). Keepalive messages are sent from one Routing Engine to the other over the fxp2 interface found on the Routing Engine. The keepalive message is received by the other host module via the fpx1 interface. A keepalive message is sent back over the fxp2 interface of the other Routing Engine. In this way, the master and the backup host subsystems exchange state information.

Figure 191: Redundancy Connection for a T320 Router or T640 Routing Node (RE-600)

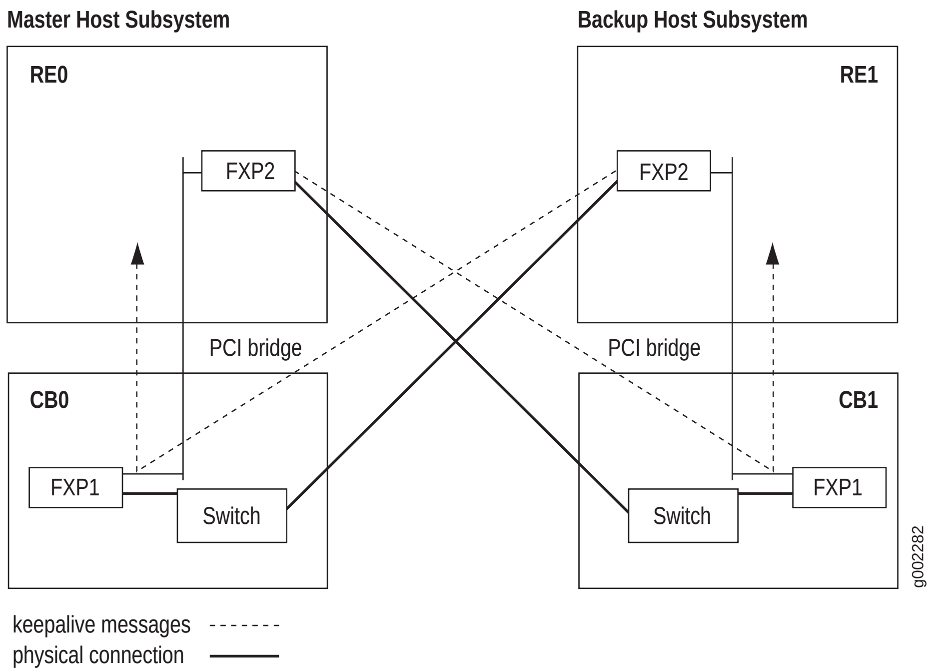
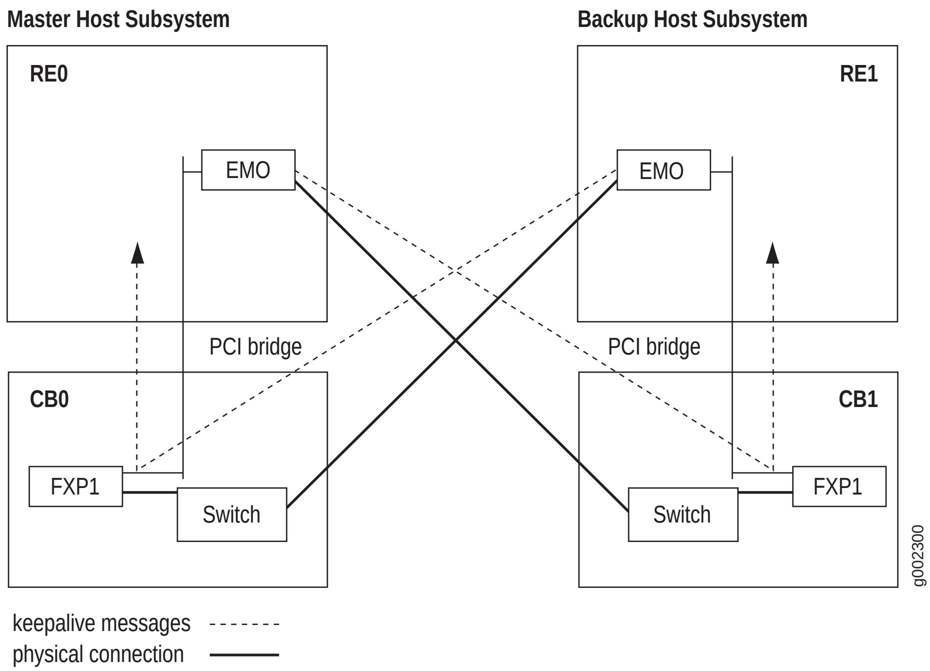


Figure 192 shows the connection between the master and backup host modules on a T320 router or a T640 routing node with a Routing Engine 1600 (RE-1600).

Figure 192: Redundancy Connection for a T320 Router or T640 Routing Node (RE-1600)



Determining Which Routing Engine You Are Logged In To

Steps To Take

1. Display Routing Engine Status on page 476
2. Display the Router Hardware on page 476

Step 1: Display Routing Engine Status

Action To determine which Routing Engine you are logged in to, use the following CLI command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine

Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 29 degrees C / 84 degrees F
    DRAM                      2048 MB
    Memory utilization          11 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     2 percent
      Interrupt                  0 percent
      Idle                      98 percent
    Model                          RE-3.0
    Serial ID                      P10865701859
    Start time                     2004-04-15 18:45:12 UTC
    Uptime                        6 days, 3 hours, 56 minutes, 8 seconds
Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 26 degrees C / 78 degrees F
    DRAM                      2048 MB
    Memory utilization          10 percent
    CPU utilization:
[...Output Truncated...]
```

What It Means The output from the show chassis hardware command indicates that you are logged in to the master Routing Engine because this command can only be used on the master Routing Engine.

If you are not logged in to the master Routing Engine, you will see the following command output:

```
user@host> show chassis hardware

error: Aborted! This command can only be used on the master routing engine.
```

Step 2: Display the Router Hardware

Action To determine which Routing Engine you are logged in to, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                65565             M320
Midplane         REV 05   710-009120   RB0662            M320 Midplane
FPM GBUS         REV 04   710-005928   HV7564            M320 Board
FPM Display      REV 05   710-009351   HY0996            M320 FPM Display
```

```
CIP              REV 04   710-005926   HV2440           M320 CIP
PEM 0            Rev 03   740-009148   QD17663          DC Power Entry Module
PEM 1            Rev 03   740-009148   QD17664          DC Power Entry Module
PEM 2            Rev 03   740-009148   QD17662          DC Power Entry Module
PEM 3            Rev 03   740-009148   QD16006          DC Power Entry Module
Routing Engine 0 REV 05   740-008883   P11123900322     RE-4.0
Routing Engine 1 REV 05   740-008883   P11123900311     RE-4.0
CB 0             REV 07   710-009115   HW8716           M320 Control Board
CB 1             REV 07   710-009115   HW8693           M320 Control Board
[...Output truncated...]
```

What it Means The output from the show chassis hardware command indicates that you are logged in to the master Routing Engine because this command can only be used on the master Routing Engine.

If you are not logged in to the master Routing Engine, you will see the following command output:

```
user@host> show chassis hardware

error: Aborted! This command can only be used on the master routing engine.
```

Determining Routing Engine Mastership

Steps To Take To determine Routing Engine mastership, follow these steps:

1. Determine the Routing Engine Mastership By Checking Status on page 477
2. Determine Routing Engine Mastership By Checking the LEDs on page 478
3. Log In To Backup Routing Engine If graceful-switchover is Configured on page 478

Step 1: Determine the Routing Engine Mastership By Checking Status

Action To determine Routing Engine mastership, use the following CLI command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine

Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 29 degrees C / 84 degrees F
    DRAM                      2048 MB
    Memory utilization          11 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     2 percent
      Interrupt                  0 percent
      Idle                      98 percent
    Model                          RE-3.0
    Serial ID                      P10865701859
```

```
    Start time                     2004-04-15 18:45:12 UTC
    Uptime                        6 days, 3 hours, 56 minutes, 8 seconds
Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 26 degrees C / 78 degrees F
    DRAM                      2048 MB
    Memory utilization          10 percent
    CPU utilization:
[...Output Truncated...]
```

What It Means The command output displays which Routing Engine is master (the one in Slot 0 RE0) and which is backup (the one in Slot 1 RE1) plus other hardware and operational status information.

Step 2: Determine Routing Engine Mastership By Checking the LEDs

Action Physically check the LEDs on either the craft interface or the Routing Engine (depending on which chassis the Routing Engine is installed). The Routing Engine that displays an illuminated Master LED is the master Routing Engine. For the location and interpretation of LEDs, see "Monitoring the Routing Engine Status" on page 136.

Step 3: Log In To Backup Routing Engine If graceful-switchover is Configured

If graceful-switchover is configured, the CLI command prompt will look as follows:

```
{backup}
user@host-re0>

{master}
user@host-re1>
```

With RE1 as master and RE0 as backup.

Action If you are logged in to the master Routing Engine, log in to the backup Routing Engine by using the following CLI command:

user@host> **request routing-engine login other-routing-engine**

Sample Output

```
user@host> request routing-engine login other-routing-engine
€Password: ########
{backup}
user@host-re0>
```

What It Means You are now logged in to the backup Routing Engine in slot RE0.

Manually Configuring Master and Backup Routing Engines

For routers with two Routing Engines, you can configure which Routing Engine is the master and which is the backup. By default, the Routing Engine in slot 0 is the master (RE0) and the one in slot 1 is the backup (RE1).

To modify the default configuration, include the routing-engine statement at the [edit chassis redundancy] hierarchy level:

```
[edit chassis redundancy]
routing-engine slot-number (master | backup | disabled);
```

slot-number can be 0 or 1. To configure the Routing Engine to be the master, specify the master option. To configure it to be the backup, specify the backup option. To switch between the master and the backup Routing Engines, you must modify the configuration and then activate it by issuing the commit command.

The running state of a Routing Engine (master, backup, or disabled) is determined by mastership election upon system boot.

- Master—If a Routing Engine is configured as master, it has full functionality. It receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components, and has full control over the chassis. Once a Routing Engine becomes master, it resets the switch plane (SSB, SCB, and SFM) and downloads its current version of the microkernel to the Packet Forwarding Engine components, guaranteeing software compatibility.

- Backup—If a Routing Engine is configured to be the backup, it does not maintain routing tables or communicate with Packet Forwarding Engine or chassis components. However, it runs through its memory check and boot sequence to the point of displaying a login prompt. A backup Routing Engine supports full management access through the Ethernet, console, and auxiliary ports, and can communicate with the master Routing Engine. Additionally, a backup Routing Engine responds to the Routing Engine request chassis routing-engine master switch command. The backup Routing Engine maintains a connection with the master Routing Engine and monitors the master Routing Engine. If the connection is broken, you can switch mastership by entering the switchover command. If the master Routing Engine is hot-swapped out of the system, the backup takes over control of the system as the new master Routing Engine. Once a Routing Engine becomes master, it resets the switch plane and downloads its own version of the microkernel to the Packet Forwarding Engine components.

- Disabled—A disabled Routing Engine has progressed through its memory check and boot sequence to the point of displaying a login prompt (similar to backup state) but does not respond to a request chassis routing-engine master switch command. A Routing Engine in disabled state supports full management access through the Ethernet, console, and auxiliary ports, and can communicate with the master Routing Engine. A disabled Routing Engine does not participate in a mastership election. To move from disabled state to backup state, the Routing Engine must be reconfigured to be the backup Routing Engine.

Action To configure RE1 to be the default master, issue the following CLI command in configuration mode at the [edit] hierarchy level:

For slot 0:

```
[edit]
user@host# set chassis redundancy routing-engine 1 master
```

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

For slot 1:

```
[edit]
user@host# set chassis redundancy routing-engine 0 backup

[edit]
user@host# commit
```

Action To view the Routing Engine mastership/backup status, use the following CLI command in operational mode:

```
user@host> show chassis routing-engine
```

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 26 degrees C / 78 degrees F
    DRAM                      2048 MB
    Memory utilization          12 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     1 percent
      Interrupt                  0 percent
      Idle                      99 percent
    Serial ID                      210929000142
    Start time                     2004-05-12 13:14:30 PDT
    Uptime                        5 days, 22 hours, 7 minutes, 9 seconds
    Load averages:                 1 minute   5 minute  15 minute
                                       0.07       0.02       0.00
Routing Engine status:
  Slot 1:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 27 degrees C / 80 degrees F
    DRAM                      2048 MB
    Memory utilization          13 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     0 percent
      Interrupt                  0 percent
      Idle                     100 percent
    Serial ID                      210929000143
    Start time                     2004-04-05 17:08:41 PDT
    Uptime                        42 days, 18 hours, 12 minutes, 45 seconds
```

What It Means Each Routing Engine only checks its own configuration. Therefore, you must configure the redundancy settings on both Routing Engines correctly for the system to operate properly.

If both Routing Engines are configured as master, whichever Routing Engine comes up first will be the master. When the second Routing Engine comes up, it will try to assume mastership. However, the current master Routing Engine will reject this request, and the second Routing Engine will become the backup.

If both Routing Engines are configured as backup and come up after bootup, neither Routing Engine becomes master. The only way for either to become master is if one of the host module components (such as the Routing Engine) is physically removed, or if a Routing Engine has failover on-loss-of-keepalives configured and the connection between Routing Engines is interrupted for a period of time. The resulting timeout due to a loss of keepalives will force one of the Routing Engines to become the master. See "Configuring the Backup Routing Engine to Assume Mastership on Failure of Keepalives" on page 485 for more information.

Manually Switching Routing Engine Mastership

Action To manually switch the Routing Engine mastership, use one of the following CLI commands.

- From the backup Routing Engine, request the backup Routing Engine to acquire mastership:

  user@host> **request chassis routing-engine master acquire**

```
user@host> request chassis routing-engine master acquire
warning: Traffic will be interrupted while the PFE is re-initialized
Attempt to become the master routing engine ? [yes,no] (no)

Resolving mastership...
Complete. The local routing engine becomes the master.
```

- From the master Routing Engine, request the backup Routing Engine to acquire mastership:

  user@host> **request chassis routing-engine master release**

```
user@host> request chassis routing-engine master release

Traffic will be interrupted while the PFE is re-initialized
Request the other routing engine become master ? [yes,no] (no)

Resolving mastership...
Complete. The other routing engine becomes the master.
```

- Switch mastership from either the backup or master Routing Engine:

  user@host> **request chassis routing-engine master switch**

If graceful-switchover is not configured, the command output looks as follows:

```
user@host> request chassis routing-engine master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between routing engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The local routing engine becomes the master.
```

```
user@host> request chassis routing-engine master switch
```

If graceful-switchover is configured the command output looks as follows:

```
Toggle mastership between routing engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The other routing engine becomes the master.
```

What It Means When you enter the request chassis routing-engine master acquire command on the backup Routing Engine, you see the following:

```
warning: Traffic will be interrupted while the PFE is re-initialized
Attempt to become the master routing engine ? [yes,no] (no).
```

The master Routing Engine gives up control of the system bus and goes into the backup state. The backup Routing Engine becomes master and restarts the Packet Forwarding Engine. You can then diagnose the original master Routing Engine for problems or prepare it for upgrade or reconfiguration. When switchover occurs, the backup Routing Engine does not run through its full boot cycle (only the packet forwarding components run through a full boot cycle).

When you enter the request chassis routing-engine master release command on the master Routing Engine, the system passes mastership to the backup Routing Engine. The master Routing Engine gives up control of the system bus and goes into the backup state. The backup Routing Engine becomes master and restarts the Packet Forwarding Engine. You can then diagnose the original master Routing Engine for problems or prepare it for upgrade or reconfiguration.

In all cases, once the switchover occurs, the new master Routing Engine reestablishes routing adjacencies, populates the routing table, and transfers forwarding table information to the Packet Forwarding Engine. When Routing Engine mastership changes, the Packet Forwarding Engine components are rebooted to reestablish communication links and download the microkernel to each component. When this occurs, forwarding is interrupted and packet buffers are flushed.

Determining Why Mastership Switched

Mastership can switch between the master Routing Engine and the backup Routing Engine for the following reasons:

- Hardware problems.
- The master Routing Engine is pulled.
- Software issues, such as a Routing Engine kernel crash.

Action View the log file /var/log/mastership for redundancy logging. This file contains hardware and software transitions to help debug auto-redundancy issues.

user@host> **show log mastership**

Table 107 lists the event codes that can be displayed in the mastership log.

Table 107: Logging Events

Event Code	Description
E_NULL = 0	The event is a null event.
E_CFG_M	The Routing Engine is configured as master.
E_CFG_B	The Routing Engine is configured as backup.
E_CFG_D	The Routing Engine is configured as disabled.
E_MAXTRY	The maximum number of tries to acquire or release mastership was exceeded.
E_REQ_C	A claim mastership request was sent.
E_ACK_C	A claim mastership acknowledgement was received.
E_NAK_C	A claim mastership request was not acknowledged.
E_REQ_Y	Confirmation of mastership is requested.
E_ACK_Y	Mastership is acknowledged.
E_NAK_Y	Mastership is not acknowledged.
E_REQ_G	A giveup mastership request was sent by a Routing Engine.
E_ACK_G	The Routing Engine acknowledges giveup of mastership.
E_CMD_A	The command request chassis routing-engine master acquire was issued from the backup Routing Engine.
E_CMD_F	Force switchover command was issued.
E_CMD_R	The command request chassis routing-engine master release was issued from the master Routing Engine.
E_CMD_S	The command request chassis routing-engine master switch was issued from a Routing Engine.
E_NO_ORE	No other Routing Engine is detected.
E_TMOUT	A request timed out.
E_NO_IPC	Routing Engine connection was lost.
E_ORE_M	Other Routing Engine state was changed to master.
E_ORE_B	Other Routing Engine state was changed to backup.
E_ORE_D	Other Routing Engine state was changed to disabled.

Sample Output

```
user@host> show log mastership
Jan 12 21:50:05  clear-log[865]: logfile cleared
Jan 12 21:50:18 failed to receive keepalives from other RE for the last 60 sec
Jan 12 21:50:23 failed to send RE info/keepalive: errno=22, total=6 in the last
20 sec
Jan 12 21:50:23 failed to send RE info/keepalive: errno=22, total=6 in the last
20 sec
Jan 12 21:50:34 event = E_CMD_R, state = master, param = 0x0 Jan 12 21:50:34
send "you are the master" request Jan 12 21:50:34 Failed to send RE mastership
cmd. err = 65 Jan 12 21:50:34 Currentstate: master  NextState:giveup
                   reason_code: 1
Jan 12 21:50:34 timestamp: Wed Jan 12 21:50:34 2000
Jan 12 21:50:34 new state = giveup
Jan 12 21:50:36 event = E_TMOUT, state = giveup, param = 0x0 Jan 12 21:50:36
send "you are the master" request
Jan 12 21:50:36 Failed to send RE mastership cmd. err = 65 Jan 12 21:50:36
```

```
Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:36 new state = giveup
Jan 12 21:50:38 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:38 send "you are the master" request
Jan 12 21:50:38 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:38 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:38 new state = giveup
Jan 12 21:50:40 failed to receive keepalives from other RE for the last 80 sec
Jan 12 21:50:41 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:41 send "you are the master" request
Jan 12 21:50:41 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:41 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:41 new state = giveup
Jan 12 21:50:43 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:43 send "you are the master" request
Jan 12 21:50:43 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:43 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:43 new state = giveup
Jan 12 21:50:46 failed to send RE info/keepalive: errno=35, total=7 in the last
20 sec
Jan 12 21:50:46 failed to send RE info/keepalive: errno=35, total=7 in the last
20 sec
Jan 12 21:50:46 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:46 send "you are the master" request
Jan 12 21:50:46 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:46 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:46 new state = giveup
Jan 12 21:50:48 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:48 send "you are the master" request
Jan 12 21:50:48 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:48 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:48 new state = giveup
Jan 12 21:50:50 event = E_TMOUT, state = giveup, param = 0x0
Jan 12 21:50:50 send "you are the master" request
Jan 12 21:50:50 Failed to send RE mastership cmd. err = 65
Jan 12 21:50:50 Currentstate: giveup  NextState:giveup
                   reason_code: 1
Jan 12 21:50:50 new state = giveup
Jan 12 21:50:53 event = E_MAXTRY, state = giveup, param = 0x0
Jan 12 21:50:53 Currentstate: giveup  NextState:master
                   reason_code: 1
Jan 12 21:50:53 timestamp: Wed
Jan 12 21:50:53 2000
Jan 12 21:50:53 new state = master
Jan 12 21:51:01 failed to receive keepalives from other RE for the last 100 sec
Jan 12 21:51:06 failed to send RE info/keepalive: errno=65, total=7 in the last
20 sec
Jan 12 21:51:06 failed to send RE info/keepalive: errno=65, total=7 in the last
20 sec
Jan 12 21:51:21 failed to receive keepalives from other RE for the last 120 sec
Jan 12 21:51:26 failed to send RE info/keepalive: errno=22, total=6 in the last
20 sec
Jan 12 21:51:26 failed to send RE info/keepalive: errno=22, total=6 in the last
20 sec
```

What It Means The beginning of the log shows that keepalives are not being responded to and the state of the Routing Engine changed from master to giveup after the request chassis routing-engine master release command was issued. However, the other Routing Engine is not taking over mastership because it is unreachable. Eventually a timeout (E_TMOUT) occurs until the Routing Engine reaches the maximum number of attempts permitted (E_MAXTRY). The output then shows the Routing Engine state changing from giveup back to master.

The output doesn't indicate why the mastership switchover did not work. However, it is clear that the backup Routing Engine is unreachable.

Configuring the Backup Routing Engine to Assume Mastership on Failure of Keepalives

Action Configure the backup Routing Engine to automatically assume mastership if it detects a loss of keepalive responses with the set chassis routing-engine statement at the [edit] hierarchy level:

[edit]
user@host# **set chassis redundancy failover on-loss-of-keepalives**

NOTE: By default, a backup Routing Engine does not assume mastership when a loss of keepalive responses occurs.

Sample Output

```
[edit]
user@host# set chassis redundancy failover on-loss-of-keepalives

[edit]
user@host# set chassis redundancy keepalive-time 300

[edit]
user@host# commit
    commit complete
```

What it Means The results of issuing this command on the backup Routing Engine are as follows:

- Every 20 seconds of keepalive loss, a message is added to the /var/log/mastership file.
- After keepalive-time passes, the backup Routing Engine attempts to claim mastership.
- When the backup Routing Engine claims mastership, it continues to be master even after the other Routing Engine configured as master has successfully resumed operation. Therefore, if the backup Routing Engine claims mastership, you must manually switch mastership.
- The default time before failover will occur is set to 300 seconds (5 minutes). You can change the default keepalive time period with the set chassis redundancy keepalive-time *time-in-seconds* command (the range for keepalive-time is from 2 to 10,000 seconds).
- Keepalive messages are sent every second.

Avoiding Redundancy Problems

Problems with reliable redundancy are more often caused by poor management of software rather than by hardware failure. The following operating guidelines reduce the likelihood of significant downtime due to Routing Engine redundancy conflicts.

Steps To Take

Step 1: Operate the Same Type of Routing Engine and JUNOS Software

The active and standby Routing Engines must be the same type of Routing Engine and must operate the same version of JUNOS software; otherwise, anomalies in operation can occur.

Step 2: Use the Groups Configuration

Action Apply a single configuration file to both Routing Engines using the groups *group-name* statement at the [edit] hierarchy level:

```
[edit]
user@host# set groups group-name
```

Where *group-name* is the name of the configuration group. To configure multiple groups, specify more than one *group-name*. On routers that support multiple Routing Engines, you can also specify two special group names:

- re0—Configuration statements that are applied to the Routing Engine in slot 0.
- re1—Configuration statements that are applied to the Routing Engine in slot 1.

The configuration specified in group re0 is only applied if the current Routing Engine is in slot 0; likewise, the configuration specified in group re1 is only applied if the current Routing Engine is in slot 1. Therefore, both Routing Engines can use the same configuration file, each using only the configuration statements that apply to it. Each re0 or re1 group contains at a minimum the configuration for the hostname and the management interface (fxp0). If each Routing Engine uses a different management interface, the group also should contain the configuration for the backup router and static routes.

To view the existing groups configuration, use the following CLI command in configuration mode:

```
[edit]
user@host# groups
user@host# show
```

Sample Output

```
[edit groups]
user@host# show
re0 {
    system {
        host-name foo-re0;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.0.0.1/24;
                }
            }
        }
    }
}
re1 {
    system {
        host-name foo-re1;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.0.0.2/24;
                }
            }
        }
    }
}
```

What it Means Use the already-existing groups statement, and use re0 and re1 as keyword group names. Each Routing Engine applies the slot-specific group configuration information to its configurations.

In the main configuration body, add the rest of the configuration that will be the same on both Routing Engines. Do not include the configuration statements that you made in the group configurations (such as configurations for fxp0). If you configure items in the body of the statement that also exist in the groups statement, the configuration in the body takes precedence—the configuration from the group statement will not be inherited.

Action Display the groups that were applied using the following configuration mode CLI command:

```
[edit]
user@host# show apply-groups
```

Sample Output

```
user@host# show apply-groups
apply-groups [ re0 re1 ];
```

Step 3: Synchronize Configurations

Action Synchronize configurations between two Routing Engines using the synchronize statement at the [edit] hierarchy level:

```
[edit]
user@host# commit synchronize
```

Sample Output

```
[edit]
root# commit synchronize
re1: configuration check succeeds
re0: configuration check succeeds
re1: commit complete
re0: commit complete
```

What it Means When this statement is selected, the configuration file is copied to the other Routing Engine, followed by a load override and a commit. No user intervention is required.

NOTE: Both Routing Engines must be running JUNOS software Release 5.1 or higher. Use the groups statement to ensure that differences in the configurations for RE0 and RE1 are applied.

Step 4: Copy a Configuration File from One Routing Engine to Another

Action You can copy a configuration file from one Routing Engine to another using the file copy command. The file is transferred through the internal Ethernet interface (FXP1 or FXP2, depending on the router):

```
user@host> file copy <source> <destination>
```

NOTE: Both Routing Engines must have jbase version 4.1 or higher loaded.

Sample Output Copy a file on RE0 to RE1:

```
user@re0> file copy /var/tmp/jinstall-6.0R3.3-domestic-signed.tgz
re1:/var/tmp1/
```

Check the result on RE1:

```
user@re1> file list /var/tmp/
.pccardd=
jbundle-5.5R3.1-domestic.tgz*
jinstall-6.0R3.3-domestic-signed.tgz
sampled.pkts
```

What it Means The file jinstall-6.0R3.3-domestic-signed.tgz is copied from RE0 to RE1.

Step 5: Use the Proper Shutdown Process on a Backup Routing Engine

Action The request system halt command only shuts down the Routing Engine you are logged in to; the other Routing Engine is still running and may be performing file management or some other task that could create anomalies.

user@re0> **request system halt**

Sample Output

```
user@re0> request system halt
warning: This command will not halt the other routing-engine.
If planning to switch off power, use the both-routing-engines option.
Halt the system ? [yes,no] (no)

*** FINAL System shutdown message from root@utah ***
System going down IMMEDIATELY


shutdown: [pid 8669]
Shutdown NOW!
```

What It Means This command only shuts down the Routing Engine you are logged in to. To shut down both Routing Engines, use the both-routing-engines option or log in to the other Routing Engine and perform the shutdown again.

Chapter 37

Monitoring Redundant Routing Engines

You monitor redundant Routing Engines to ensure that system processes function normally, such as routing protocols, packet forwarding tables, router interfaces, system management, JUNOS software and file system storage, and monitoring functions. (See Table 108.)

This chapter describes how to monitor redundant Routing Engines. For more information about monitoring Routing Engines, see "Monitoring the Routing Engine" on page 125. See also the applicable router hardware installation guide.

Table 108: Checklist for Monitoring Redundant Routing Engines

Monitor Redundant Routing Engine Tasks	Command or Action
Understanding Redundant Routing Engines on page 493	
Redundant Routing Engine Characteristics on page 493 ■ M10i Router Routing Engine Redundancy on page 494 ■ M20 Router Routing Engine Redundancy on page 495 ■ M40e and M160 Router Routing Engine Redundancy on page 496 ■ M320 Router Routing Engine Redundancy on page 497 ■ T320 Router and T640 Routing Node Routing Engine Redundancy on page 498	
Understanding the Redundant Routing Engine Configuration on page 500	[edit] [edit chassis redundancy] show or show chassis redundancy
Understanding Redundant Routing Engine Automatic Failover on page 501	
Understanding the Default Routing Engine Redundancy Behavior on page 501	
Displaying the Redundant Routing Engines Installed in the Router on page 502	show chassis hardware show chassis routing-engine
Checking the Redundant Routing Engine Status on page 503	See "Monitoring the Routing Engine Status" on page 136.
Displaying Redundant Routing Engine Mastership and Backup on page 503	show chassis routing-engine
Displaying Redundant Routing Engine Errors on page 504	show log mastership

Monitor Redundant Routing Engine Tasks	Command or Action
Manually Switching from Master to Backup Routing Engine on page 504	request chassis routing-engine master release request chassis routing-engine master switch
Replacing a Redundant Routing Engine on page 506	See "Removing a Routing Engine" on page 161.

See Also

- Monitoring the Host Module on page 341
- Monitoring the Routing Engine on page 125
- Monitoring the MCS on page 359
- Host Redundancy Overview on page 463
- Monitoring Redundant MCSs on page 567
- Monitoring Redundant Control Boards on page 559

Understanding Redundant Routing Engines

Purpose Inspect redundant Routing Engines to minimize system process failures.

What Are Redundant Routing Engines Redundant Routing Engines are two Routing Engines that are installed in the same router. One functions as the master, while the other stands by as a backup should the master Routing Engine fail. By default, the Routing Engine in slot 0 is the master (RE0) and the one in slot 1 is the backup (RE1).

Redundant Routing Engine Characteristics

Table 109 describes redundant Routing Engine characteristics for routing platforms.

Table 109: M-series Platform Redundant Routing Engine Characteristics

Component	M10i	M20	M40	M40e	M160	M320	T320/ T640
Redundant Routing Engine	X	X					
Redundant host modules with Routing Engine and MCS				X	X		
Redundant host subsystems with Routing Engine and Control Board						X	
Redundant host modules with Routing Engine and Control Board							X

The following sections describe the various routing platform Routing Engines:

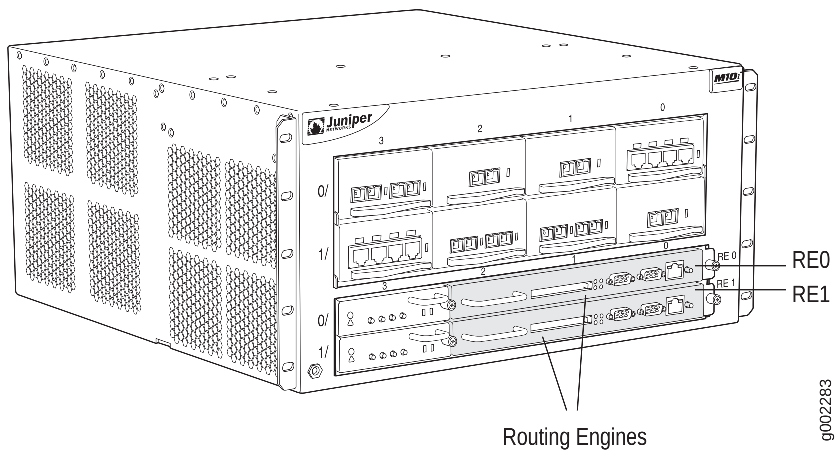
- M10i Router Routing Engine Redundancy on page 494
- M20 Router Routing Engine Redundancy on page 495
- M40e and M160 Router Routing Engine Redundancy on page 496
- M320 Router Routing Engine Redundancy on page 497
- T320 Router and T640 Routing Node Routing Engine Redundancy on page 498

M10i Router Routing Engine Redundancy

The M10i router has redundant Routing Engines. The M10i router has one Routing Engine in slot RE0 and another in slot RE1 (see Figure 193). By default, the Routing Engine in slot RE0 is the master and the one in slot RE1 is the backup. If one Routing Engine fails, the other one assumes the routing functions.

The M10i router Routing Engine faceplate has LEDs that indicate redundant Routing Engine operating status and mastership. (See "Check the M10i Router Routing Engine LEDs" on page 139.)

Figure 193: M10i Router Redundant Routing Engine

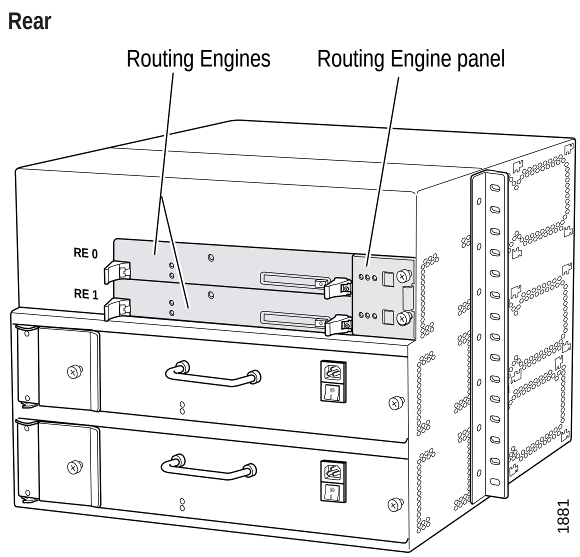


M20 Router Routing Engine Redundancy

The M20 router has one Routing Engine in slot RE0 and another in slot RE1 (see Figure 194). By default, the Routing Engine in slot RE0 is the master and the one in slot RE1 is the backup. If one Routing Engine fails, the other one assumes the routing functions.

The M20 router Routing Engine panel has LEDs that indicate redundant Routing Engine operating status and mastership. The craft interface also has LEDs that indicate redundant Routing Engine status and mastership. (See "Check the M20 Router Routing Engine LEDs" on page 140.)

Figure 194: M20 Router Redundant Routing Engine



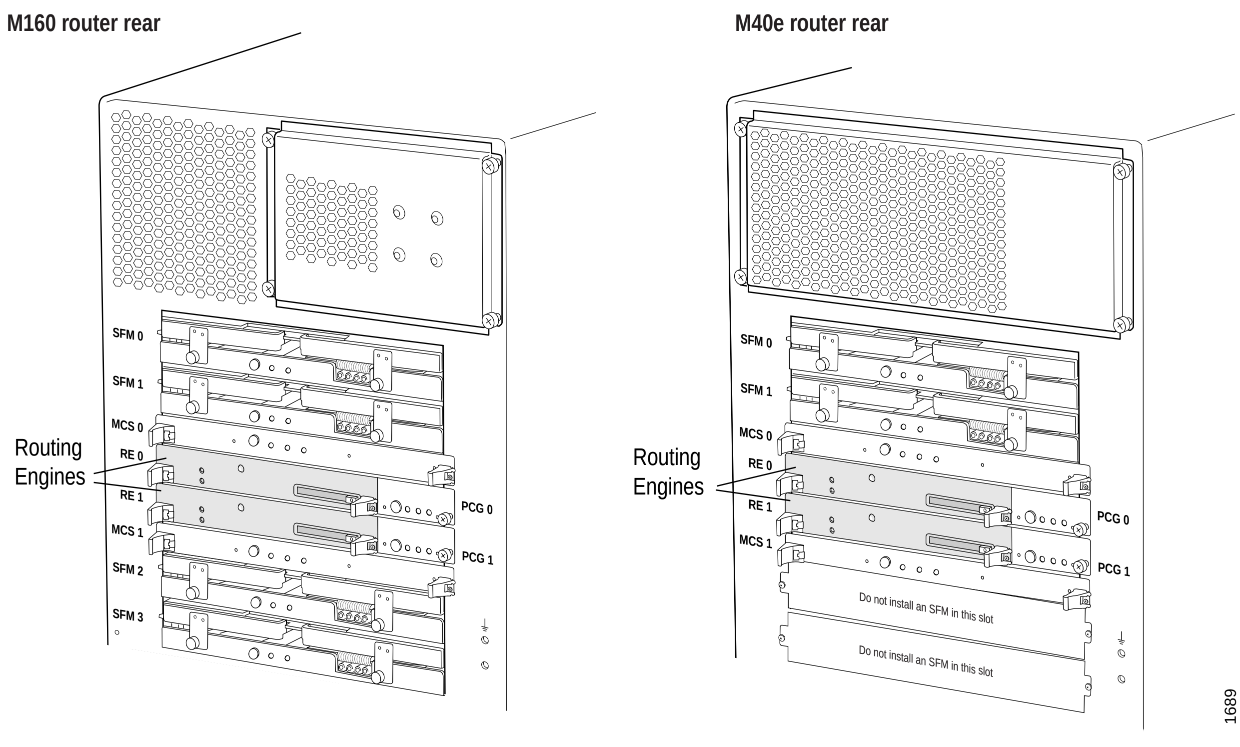
M40e and M160 Router Routing Engine Redundancy

The M40e and M160 routers have redundant Routing Engines that are components of the host module (see Figure 195). The host module consists of a Routing Engine and a Miscellaneous Control Subsystem (MCS). You can install two host modules in the M40e and M160 routers. For more information about monitoring redundant MCSs, see "Monitoring Redundant MCSs" on page 567.

Both the Routing Engine and the MCS must be installed for the host module to function. When two host modules are installed in the router, both are powered on, but only one is the master; the second host module is the backup and performs no functions. By default, the master host module has components installed in slots RE0 and MCS0; the backup host module has components installed in slots RE1 and MCS1.

The M40e and M160 router craft interface LEDs indicate the Routing Engine operating status and mastership. (See "Check the M40e and M160 Router Routing Engine LEDs" on page 143.)

Figure 195: M40e and M160 Router Redundant Routing Engines



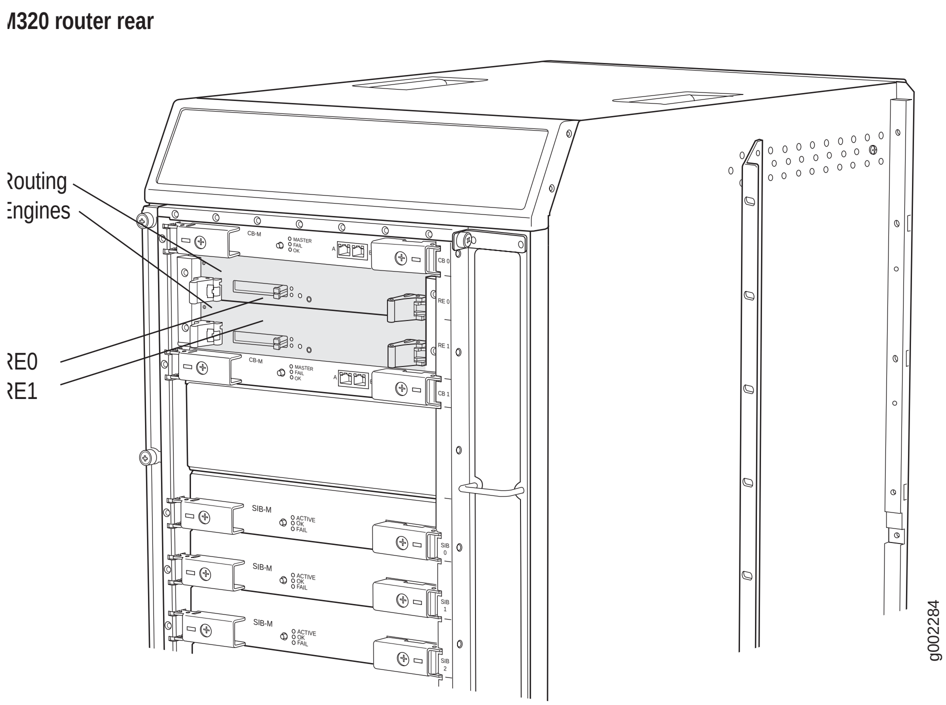
M320 Router Routing Engine Redundancy

The M320 router has a redundant Routing Engine that is a component of the host subsystem (see Figure 196). The host subsystem consists of a Routing Engine and a Control Board. Two host subsystems can be installed in the M320 router. For more information about monitoring redundant Control Boards, see "Monitoring Redundant Control Boards" on page 559.

Both the Routing Engine and the Control Board must be installed for the host subsystem to function. When two host subsystems are installed in the router, both are powered on, but only one is the master; the second host subsystem is the backup and performs no functions. By default, the master host module has components installed in slots RE0 and CB0; the backup host module has components installed in slots RE1 and CB1. The Routing Engines are hot-pluggable.

The M320 router craft interface LEDs indicate the Routing Engine operating status and mastership. (See "Check the M320 Router Routing Engine LEDs" on page 144.)

Figure 196: M320 Router Redundant Routing Engines



T320 Router and T640 Routing Node Routing Engine Redundancy

Figure 197 shows the T320 router redundant Routing Engines that are components of the host subsystem.

Figure 197: T320 Router Routing Engines

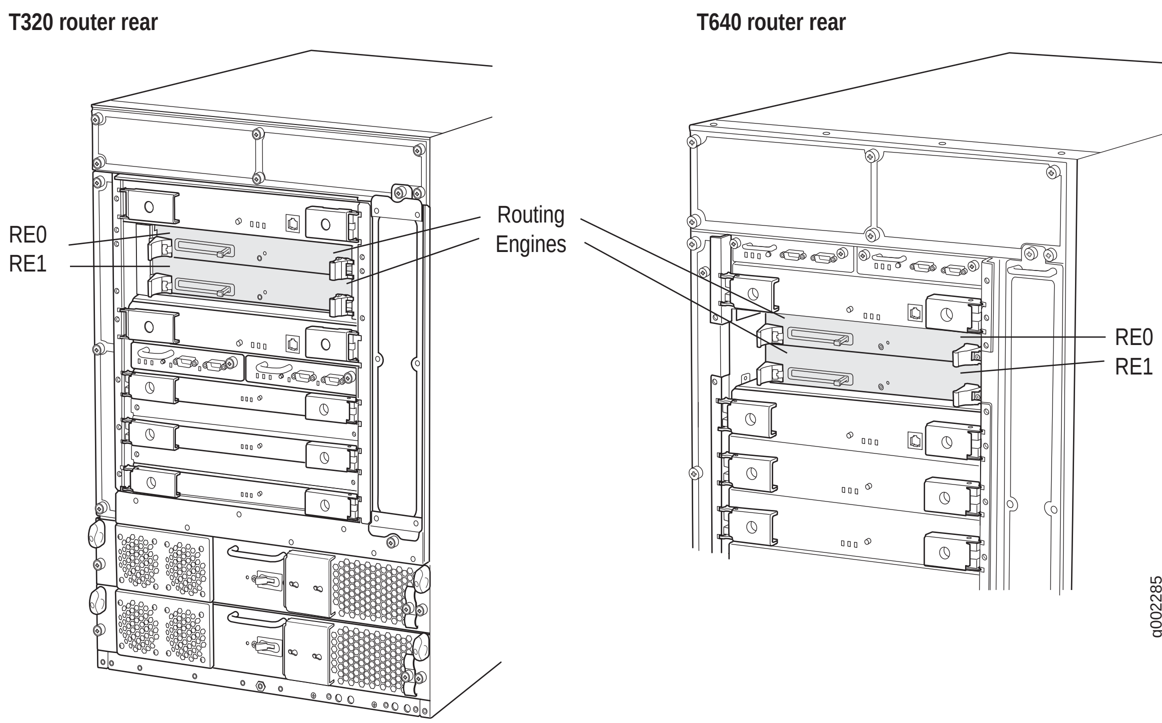
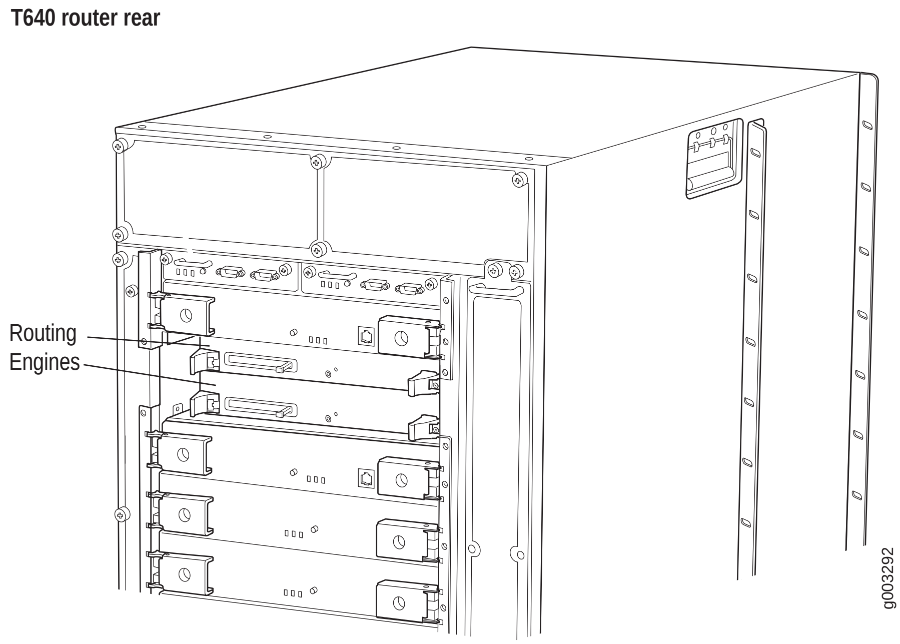


Figure 198 shows the T640 routing node redundant Routing Engines that are components of the host subsystem.

Figure 198: T640 Routing Node Routing Engines



The host subsystem consists of a Routing Engine and a Control Board. You can install two host subsystems in the T320 router and T640 routing node. For more information about monitoring redundant Control Boards, see “Monitoring Redundant Control Boards” on page 559.

Both the Routing Engine and the Control Board must be installed for the host subsystem to function. When two host subsystems are installed in the router, both are powered on, but only one is the master; the second host subsystem is the backup and performs no functions. By default, the master host subsystem has components installed in slots RE0 and CB0; the backup host module has components installed in slots RE1 and CB1. If one Routing Engine physically fails, the other one assumes the routing functions. If a software failure occurs, the other backup Routing Engine assumes routing functions if some preliminary configuration has been done. For more information, see“Host Redundancy Overview” on page 463.

The T320 router and T640 routing node craft interface LEDs indicate the Routing Engine operating status and mastership. (See “Check the T320 Router Routing Engine LEDs” on page 144 and “Check the T640 Routing Node Routing Engine LEDs” on page 145.)

Understanding the Redundant Routing Engine Configuration

For routers with redundant Routing Engines, you can configure a master and backup Routing Engine. By default, the Routing Engine in slot RE0 is the master, and the Routing Engine in slot RE1 is the backup. Once configured, you can specify the Routing Engine to assume mastership automatically if it detects loss of the keepalive signal from the master. You can configure Routing Engine redundancy is in the JUNOS software command-line interface (CLI) configuration mode at the [edit chassis redundancy] hierarchy level.

NOTE: We recommend that both Routing Engines have the same configuration. When changing the configuration on a Routing Engine, commit it to both Routing Engines using the commit synchronize statement at the [edit] hierarchy level. For more information about synchronizing configurations, see "Host Redundancy Overview" on page 463.

You can configure redundant Routing Engine automatic failover for the backup Routing Engine with a specified failover time. By default, automatic failover is disabled. To enable it, include the failover on-loss-of-keepalives statement at the [edit chassis redundancy] hierarchy level. By default, failover will occur after 300 seconds (5 minutes) unless a different time is specified. The failover time is indicated by the *keepalive-timeseconds* statement at the [edit chassis redundancy] hierarchy level. The range for the keepalive time is from 2 to 10,000 seconds.

To display the current Routing Engine redundancy configuration, follow these steps:

1. Enter the CLI configuration mode using the following command:

   user@host# **configure**

2. From the [edit chassis redundancy] hierarchy level, show the configuration using the following command:

   user@host# **show**

Alternative Action To display the current Routing Engine configuration, you can also use the following CLI command:

user@host> **show chassis redundancy**

Sample Output

```
user@host> show chassis redundancy
routing-engine 0 master;
routing-engine 1 backup;
failover on-loss-of-keepalives;
keepalive-time 300;
```

Understanding Redundant Routing Engine Automatic Failover

If the keepalive time is configured for 2 seconds, the sequence of events is as follows:

1. After 2 seconds of keepalive loss, a message is logged.
2. After 2 seconds of keepalive loss, the backup Routing Engine attempts to assume mastership. An alarm is generated whenever the backup Routing Engine is active, and the display is updated with the current status.
3. Once the backup Routing Engine assumes mastership, it continues to function as master even after the originally configured master Routing Engine has successfully resumed operation. You must manually restore it to its previous backup status. However, if at any time one of the Routing Engines is not present, the other Routing Engine becomes master automatically, regardless of how redundancy is configured.

Understanding the Default Routing Engine Redundancy Behavior

By default, the JUNOS software uses RE0 as the master Routing Engine and RE1 as the backup Routing Engine. Unless otherwise specified in the configuration, RE0 will always assume mastership if the acting master Routing Engine is rebooted.

To see how the default Routing Engine redundancy setting works, follow these steps:

WARNING: Do not try this procedure on a production network.

1. Make sure the router is running on RE0 as the master Routing Engine (see “Displaying Redundant Routing Engine Mastership and Backup” on page 503).
2. To manually switch the state of the Routing Engine mastership, use the request chassis routing-engine master command. RE0 is now the backup Routing Engine and RE1 is the master Routing Engine. If you use this command to change the master Routing Engine, and then restart the chassis software for any reason, the master reverts to the default setting. For information about switching Routing Engine mastership, see the request chassis routing-engine master command in the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

NOTE: On the next reboot of the master Routing Engine, the JUNOS software returns the router to the default state because you have not configured the Routing Engines to maintain this state after a reboot.

3. Reboot the master Routing Engine RE1. When you do this, the Routing Engine boots up and reads the configuration. If you have not specified in the configuration which Routing Engine is the master, RE1 uses the default configuration as the backup. Now both RE0 and RE1 are in a backup state. The JUNOS software detects this conflict and, to prevent a no-master state, reverts to the default configuration with RE0 assuming mastership.

Displaying the Redundant Routing Engines Installed in the Router

Action To determine whether a router has redundant Routing Engines, use the following CLI command:

user@host> **show chassis hardware**

NOTE: If the show chassis hardware CLI command displays no hardware information, check to see which Routing Engine you are logged in to. If you are logged in to the backup Routing Engine, no hardware information is displayed or there are errors.

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                22196             M20
Backplane        REV 07   710-001517   AL2873
Power Supply A   REV 04   740-001466   001043            DC
Power Supply B   REV 04   740-001466   000671            DC
Display          REV 04   710-001519   AJ7282
Host 0                                 c800000749a9db01  Present
Host 1                                 9a00000749b14301  Present
[...Output truncated...]
```

What It Means The command output displays the Routing Engine slot number, revision level, part number, serial number, and type.

Alternative Action To display more detailed information about the Routing Engines installed in a router, use the following CLI command:

user@host> **show chassis routing-engine**

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 29 degrees C / 84 degrees F
    DRAM                       768 Mbytes
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     1 percent
      Interrupt                  0 percent
      Idle                      98 percent
    Serial ID                      c800000749a9db01
    Start time                     2002-06-18 13:53:12 UTC
    Uptime                         70 days, 52 minutes, 40 seconds
    Load averages:                 1 minute   5 minute  15 minute
                                       0.08       0.02       0.01
Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 30 degrees C / 86 degrees F
    DRAM                  805306368 Mbytes
```

```
CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                      99 percent
Serial ID                      9a00000749b14301
Start time                     2002-06-18 13:54:05 UTC
Uptime                         70 days, 51 minutes, 50 seconds
```

Checking the Redundant Routing Engine Status

Action For more information about monitoring Routing Engine status, see "Monitoring the Routing Engine Status" on page 136.

Displaying Redundant Routing Engine Mastership and Backup

Action To display which Routing Engine is master and backup, use the following CLI command:

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status
 Slot 0
  Current state: Master
  Election priority: Master
 Temperature               41 C / 105 degrees F
  DRAM                      765 Mbytes
  CPU utilization
    User                      0 percent
    Background                0 percent
    Kernel                    0 percent
    Interrupt                 0 percent
    Idle                    100 percent
  Serial ID                    39000004f8bdec01
  Start time                    2000-01-04 22:02:58 UTC
  Uptime                        14 hours, 45 minutes, 40 seconds
  Load averages                 1 minute   5 minute  15 minute
                                     0.05      0.04      0.01
 Slot 1
  Current state   Backup
  Election priority   Backup (default)
  Temperature                41 C / 105 degrees F
[...Output truncated...]
```

What It Means The command output shows the status of the Routing Engines: RE0 is Master and RE1 is Backup.

Alternative Actions You can also use the show chassis environment routing-engine command; for more information see "Monitoring the Routing Engine Status" on page 136. The Current State field indicates which Routing Engine is master and which is backup.

For M40e and M160 routers, you can also use the show chassis craft-interface command. The command output shows the master and backup Routing Engine LED status; for more information, see "Monitoring the Routing Engine Status" on page 136.

Displaying Redundant Routing Engine Errors

Action To view redundancy log messages, use the following CLI command:

user@host> **show log mastership**

Sample Output

```
user@host> show log mastership
[...Output truncated...]
May 13 11:18:31 RE mastership msg error: subtype 52
May 13 11:18:32 failed to receive loss of keepalives from other RE for the last
20 sec
[...Output truncated...]
```

What It Means The /var/log/mastership file records error messages from redundancy logging. The file records the time of the message and a description of the message. A message is logged after 20 seconds of keepalive loss.

Manually Switching from Master to Backup Routing Engine

Action To manually switch from master to backup Routing Engine, or to force the backup Routing Engine to become master, use the following CLI command:

user@host> **request chassis routing-engine master release**

You can also use the following CLI command:

user@host> **request chassis routing-engine master switch**

For routers with multiple Routing Engines only, you can control which Routing Engine is the master.

WARNING: For routers that have two Routing Engines, both Routing Engines must be running JUNOS Release 4.0 or later. Do not run JUNOS Release 3.4 on one of the Routing Engines and Release 4.0 on the other. JUNOS software Release 3.4 does not support Routing Engine redundancy. If you are using this release of the software, only one Routing Engine can be installed in either slot in the router.

By default, the Routing Engine in slot 0 (RE0) is the master and the Routing Engine in slot 1 (RE1) is the backup. To change the default master Routing Engine, include the routing-engine statement at the [edit chassis redundancy] hierarchy level in the configuration. For more information, see the *JUNOS System Basics Configuration Guide*.

When you force the backup Routing Engine to become the master Routing Engine with the request chassis routing-engine master command and then restart the chassis software for any reason, the master reverts to the default setting.

NOTE: The configurations on the two Routing Engines do not have to be the same, and they are not automatically synchronized. If you configure both Routing Engines as masters, when the chassis software restarts for any reason, the Routing Engine in slot 0 becomes the master and the Routing Engine in slot 1 becomes the backup.

We recommend making both configurations the same.

When both Routing Engines have the same configuration and come up at the same time, the Routing Engine in slot 0 takes precedence over the Routing Engine in slot 1. Table 110 indicates which Routing Engine becomes master based on the configuration of both Routing Engines.

Table 110: Routing Engine Mastership Election

		Slot 0 Configuration		
		Master	**Backup**	**Disabled**
Slot 1 Configuration	**Master**	Slot 0: master Slot 1: backup	Slot 0: backup Slot 1: master	Slot 0: disabled Slot 1: master
	Backup	Slot 0: master Slot 1: backup	Slot 0: master Slot 1: backup	Slot 0: disabled Slot 1: master
	Disabled	Slot 0: master Slot 1: disabled	Slot 0: master Slot 1: disabled	Slot 0: disabled Slot 1: disabled

Sample Output

The following command output displays when you attempt to have the backup Routing Engine become master:

```
user@M20-host> request chassis routing-engine master acquire

warning: Traffic will be interrupted while the PFE is re-initialized

warning: The other routing engine's file system could be corrupted
Reset other routing engine and become master ? [yes,no] (no)
```

The following command output displays when you switch the mastership from the master Routing Engine to the backup:

```
user@m20-host-0> request chassis routing-engine master switch

warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between Routing Engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The other Routing Engine becomes the master.
root@m20-host-0>
```

The following command output displays when you switch the mastership from the backup to the master Routing Engine:

```
root@m20-host-0> request chassis routing-engine master switch

warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between routing engines ? [yes,no] (no) yes

Resolving mastership...
Complete. The local routing engine becomes the master.
root@m20-host-0>
```

What It Means The command output indicates that traffic will be interrupted during the Routing Engine mastership switch process. The command output confirms whether you really want to continue with the mastership switch process, and indicates when the mastership switch process is complete.

Syntax request chassis routing-engine master <acquire <no-confirm>| release | switch>

acquire—(Optional) Attempt to become the master Routing Engine.

no-confirm—(Optional) Do not request confirmation.

release—(Optional) Request the other Routing Engine to become the master.

switch—(Optional) Toggle mastership between Routing Engines.

Replacing a Redundant Routing Engine

If you have a router with two Routing Engines and you want to shut the power off to the router or remove a Routing Engine, you must first halt the backup Routing Engine (if it has been upgraded), then halt the master Routing Engine. To halt a Routing Engine, issue the request system halt command. You can also halt both Routing Engines at the same time by issuing the request system halt both-routing-engines command.

NOTE: When you halt both Routing Engines, a message displays to press Enter to restart or to halt. If you press Enter on the master Routing Engine to restart, it will restart. However the backup Routing Engine will not restart. It will wait at the message to restart or to halt. You then have to press Enter on the console of the backup Routing Engine for it to restart.

Action To replace a redundant Routing Engine, see “Removing a Routing Engine” on page 161.

Chapter 38

Monitoring Redundant Power Supplies

You monitor and maintain redundant power supplies to ensure that power is distributed to the router components without interruption. (See Table 111.)

Table 111: Checklist for Monitoring Redundant Power Supplies

Monitor Redundant Power Supply Tasks	Command or Action
Understanding Redundant Power Supplies on page 508 ■ M5/M10 Router Redundant Power Supplies on page 508 ■ M7i Router Redundant Power Supplies on page 509 ■ M10i Router Redundant Power Supplies on page 510 ■ M20 Router Redundant Power Supplies on page 511 ■ M40 Router Redundant Power Supplies on page 512 ■ M40e Router Power Supplies nand Location on page 513 ■ M160 Router Redundant Power Supplies on page 515 ■ M320 Router Redundant Power Supplies on page 516 ■ T320 Router Redundant Power Supplies on page 517 ■ T640 Routing Node Redundant Power Supplies on page 518	
Displaying Redundant Power Supplies Installed In The Router on page 519	show chassis hardware
Checking the Redundant Power Supply Status on page 521	For more information about monitoring power supplies, see "Checking the Power Supply Status" on page 230.
Checking for Power Supply Alarms on page 521	For more information about checking for power supply alarms, see "Checking for Power Supply Alarms" on page 235.
Verifying Power Supply Failure on page 521	
Getting Power Hardware Information on page 521	For more information about removing a power supply, see "Replacing the Power Supplies" on page 250.
Replacing a Power Supply on page 521	

See Also ■ Monitoring Power Supplies on page 217

Understanding Redundant Power Supplies

Purpose Inspect redundant power supplies to ensure that they distribute power to the other router components according to their voltage requirements.

What Are Redundant Power Supplies With redundant power supplies, two power supplies are installed in a router and perform load sharing during normal operation. When one power supply fails or is switched off, the other power supply immediately and automatically assumes the entire electrical load. Table 112 lists some router characteristics for each M-series router platform type.

The power supplies are internally connected to the midplane, which delivers the power input from the circuit breaker box and distributes the different output voltages produced by the power supplies to the router's components, depending on their voltage requirements.

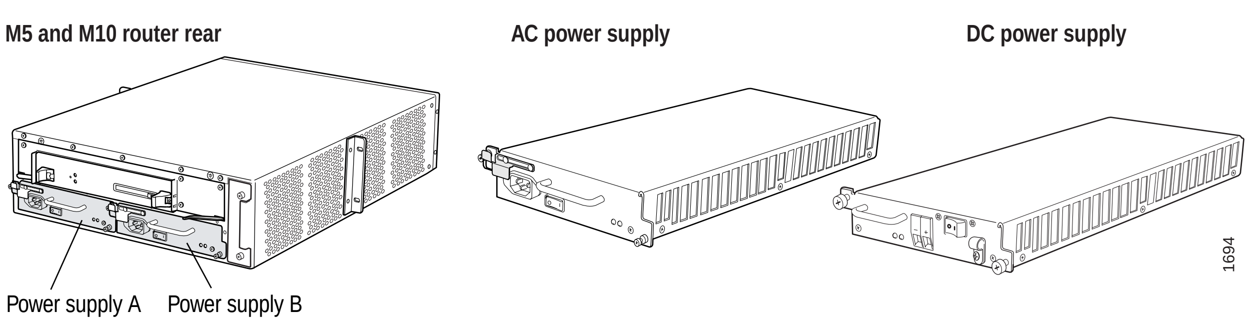
Table 112: Router Power Supply Characteristics Per Routing Platform

Power Supply Characteristic	M5/ M10	M7i/ M10i	M20	M40	M40e	M160	M320	T320	T640
Number. of power supplies	2	2/4	2	2	2	2	4	2	2
Watts per AC/DC power supply	434 W	AC 293 W DC DC 293 W	750 W	1500 W	AC 2900 W DC 3000 W	DC original 2600 W DC enhanced 3200 W	AC 1750 W DC 2000 W	3200 W DC enhanced 3200 W	6500W DC enhanced 3200 W
Supports both AC and DC power supplies	Yes	Yes	Yes	Yes	Yes	No; original or enhanced DC only	Yes	No DC only	No DC only

M5/M10 Router Redundant Power Supplies

Two load-sharing, isolated power supplies are located at the bottom rear of the M5 and M10 router chassis. The routers use either AC or DC power. Figure 199 shows the M5 and M10 router power supplies and where they are installed in the chassis.

Figure 199: M5 and M10 Router Redundant Power Supplies



When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supply instantly begins providing all the power the router needs for normal functioning and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported. The two power supplies must be either both AC or both DC.

When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

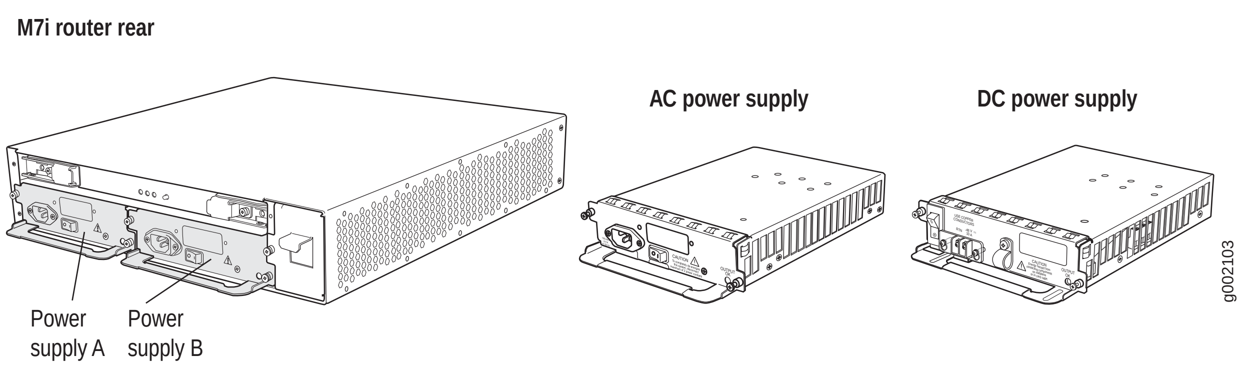
M7i Router Redundant Power Supplies

Two load-sharing, isolated power supplies are located at the bottom rear of the M7i router chassis. The router uses either AC or DC power. Figure 200 shows the M7i router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load.

For full redundancy, two power supplies are required. If a power supply stops functioning for any reason, the second power supply instantly begins providing all the power the router needs for normal functioning. The second power supply can provide full power indefinitely.

Figure 200: M7i Router Redundant Power Supplies



NOTE: When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

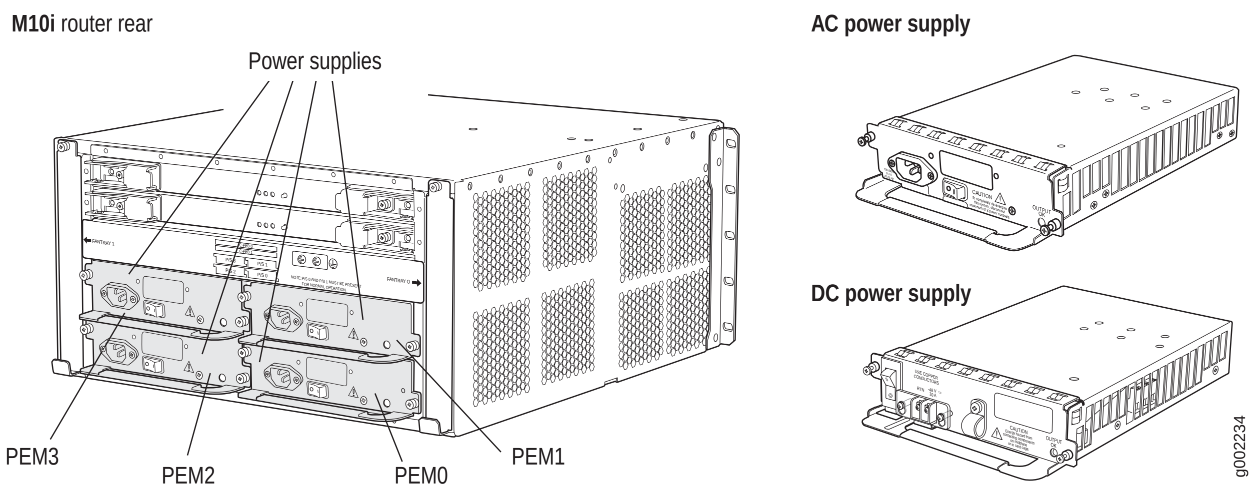
M10i Router Redundant Power Supplies

The M10i router uses either AC or DC power. You can install up to four load-sharing power supplies at the bottom rear of the chassis. Figure 201 shows the M10i router power supplies and where they are installed in the chassis.

The AC power supplies are fully redundant. If one power supply fails or is removed, the remaining power supplies instantly assume the entire electrical load. Two power supplies can provide full power for as long as the router is operational. Three power supplies are required for redundancy. Power supplies must be present in slots P/S 0 and P/S 1 for the router to operate.

The DC power supplies are fully redundant. The DC power supplies in slots P/S 0 and P/S 1 can provide full power to the router. Likewise, the DC power supplies in slots P/S 2 and P/S 3 can also provide full power. The DC power supplies in slots P/S 2 and P/S 3 jointly serve as the backup to the DC power supplies in slots P/S 0 and P/S 1. Power supplies must be present in slots P/S 0 and P/S 1 for the router to operate.

Figure 201: M10i Router Redundant Power Supplies



NOTE: AC and DC power supplies are required in slots P/S 0 and P/S 1 for the router to operate.

The DC power supplies in slots P/S 0 and P/S 1 must be powered by dedicated power feeds derived from feed A, and the DC power supplies in slots P/S 2 and P/S 3 must be powered by dedicated power feeds derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

M20 Router Redundant Power Supplies

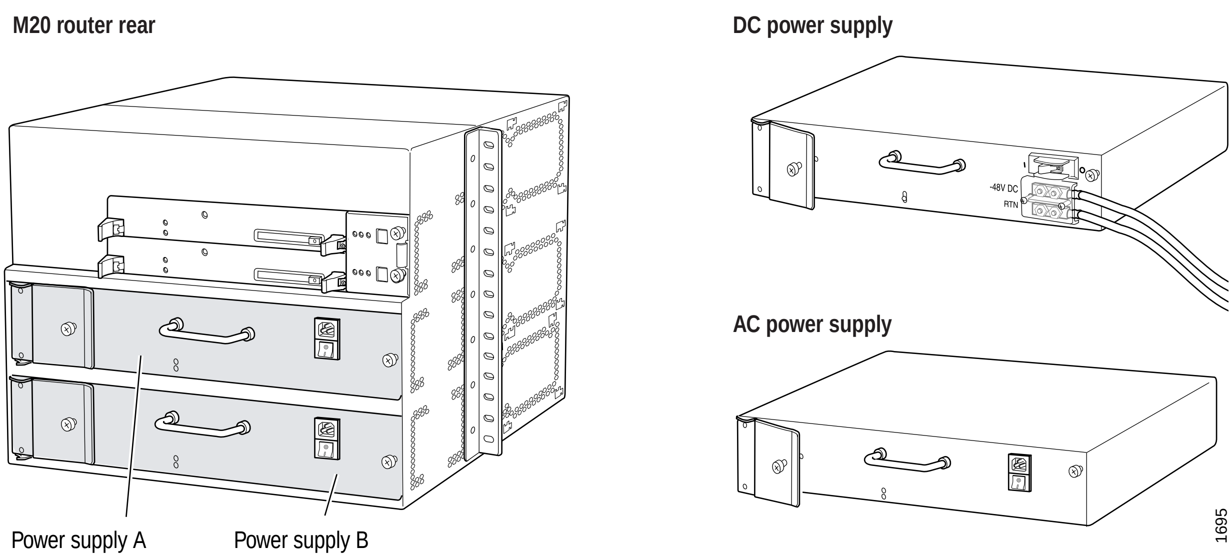
Two load-sharing, isolated power supplies are located at the bottom rear of the M20 router chassis.The router uses either AC or DC power. Figure 202 shows the M20 router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported. The two power supplies must be either both AC or both DC.

When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers and on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

Figure 202: M20 Router Redundant Power Supplies

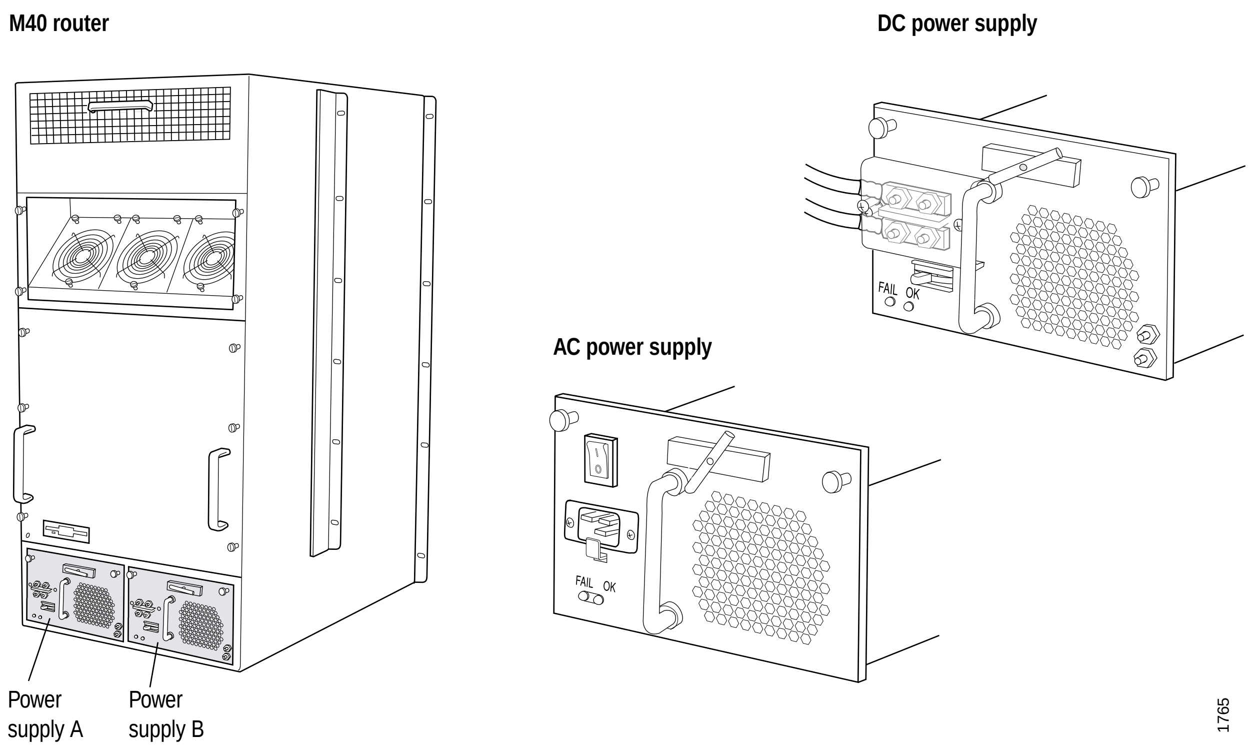


M40 Router Redundant Power Supplies

The M40 router can use either AC or DC power. Two load-sharing power supplies install into the bays located at the bottom rear of the chassis. As viewed from the rear of the chassis, the supply on the left is referred to as supply A and the supply on the right as supply B. Figure 203 shows the M40 router power supplies and where they are installed in the chassis.

The power supplies are fully redundant. When both power supplies are operational, they automatically share the electrical load. If one power supply stops functioning for any reason, the remaining power supply instantly begins providing all the power the router needs for normal functioning, and can provide full power indefinitely.

Figure 203: M40 Router Redundant Power Supplies



M40e Router Power Supplies nand Location

The M40e router uses either AC or DC power. Two load-sharing, pass-through power supplies are located at the bottom rear of the chassis. Figure 204 on page 514 shows the M40e router power supplies and where they are installed in the chassis.

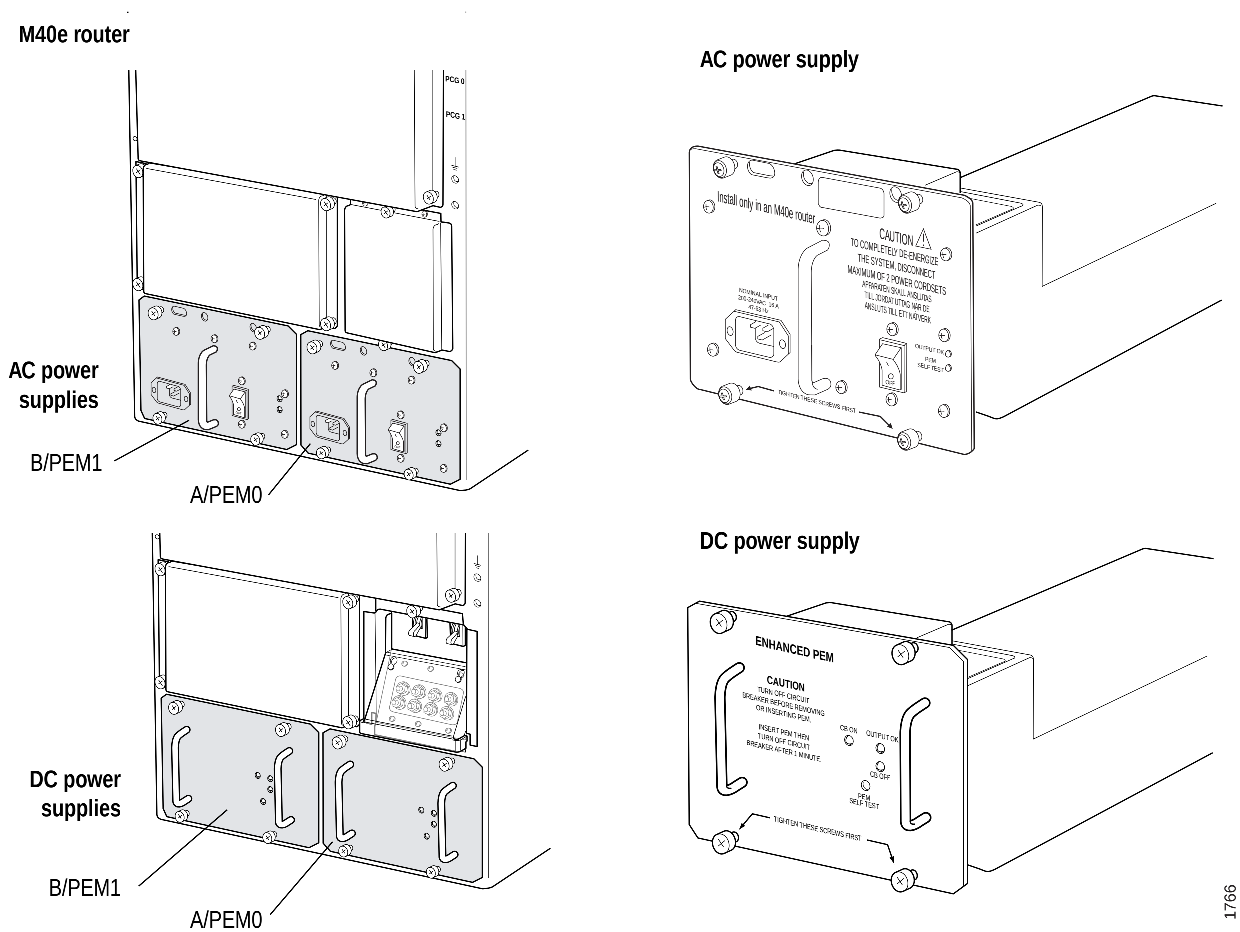
When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

NOTE: Mixing AC and DC power supplies is not supported and prevents the router from booting. If two power supplies are installed, they must be either both AC or both DC.

- A circuit breaker box must be installed on a DC-powered router, while a circuit breaker is incorporated into each AC power supply. Converting the router from AC to DC power or vice versa involves removing or installing the circuit breaker box. Only authorized service personnel should perform the conversion: this manual does not include instructions.

- When two power supplies are installed, at least one Routing Engine and one FPC must also be installed for both power supplies to power on. In the absence of this minimum load, only one power supply starts. (The router powers on and operates correctly with one power supply, but without the redundancy benefit of having a second power supply installed.)

Figure 204: M40e Router Redundant Power Supplies

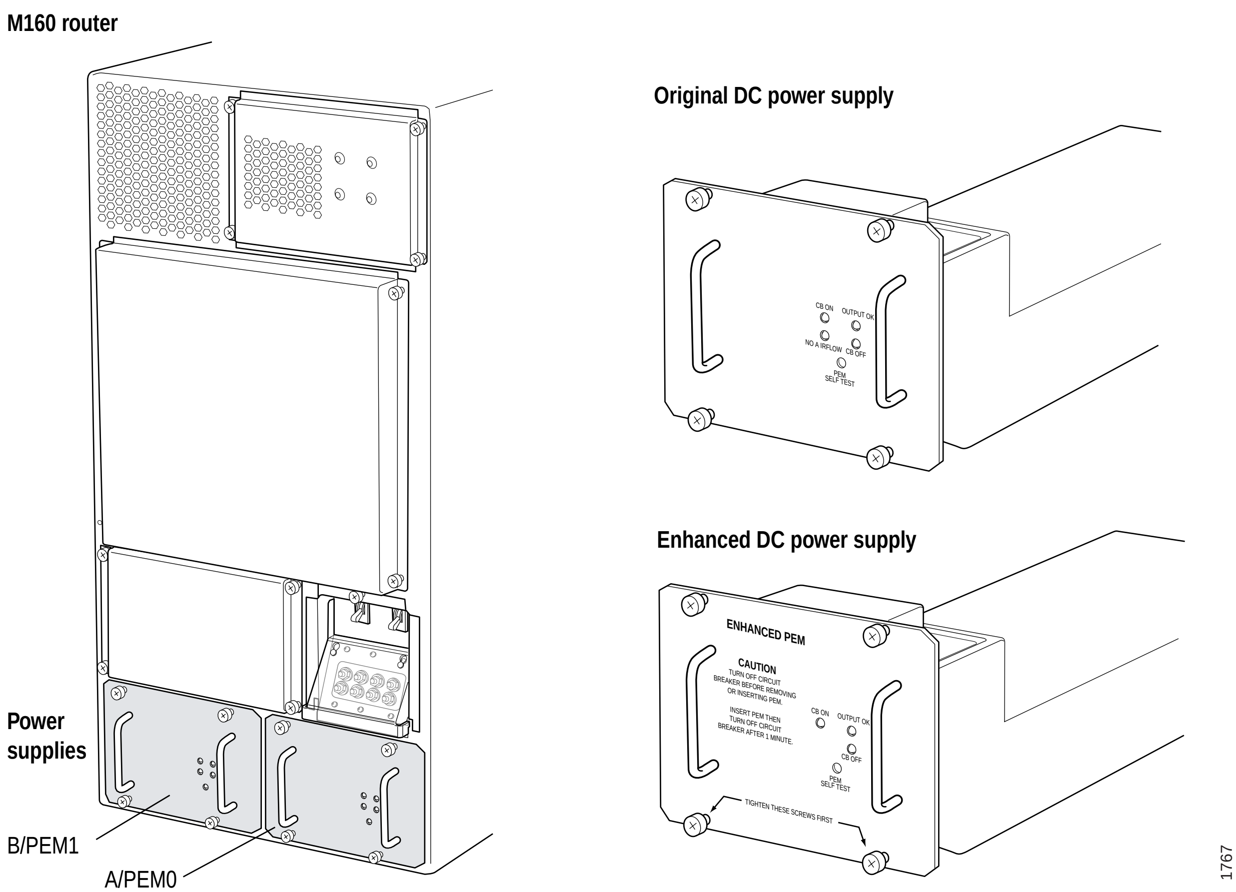


M160 Router Redundant Power Supplies

The M160 router uses DC power. Two load-sharing, pass-through power supplies are located at the bottom rear of the chassis. Figure 205 shows the M160 router power supplies and where they are installed in the chassis.

When the power supplies are installed and operational, they automatically share the electrical load. If a power supply stops functioning for any reason, the remaining power supplies instantly begin providing all the power the router needs for normal functioning, and can provide full power indefinitely.

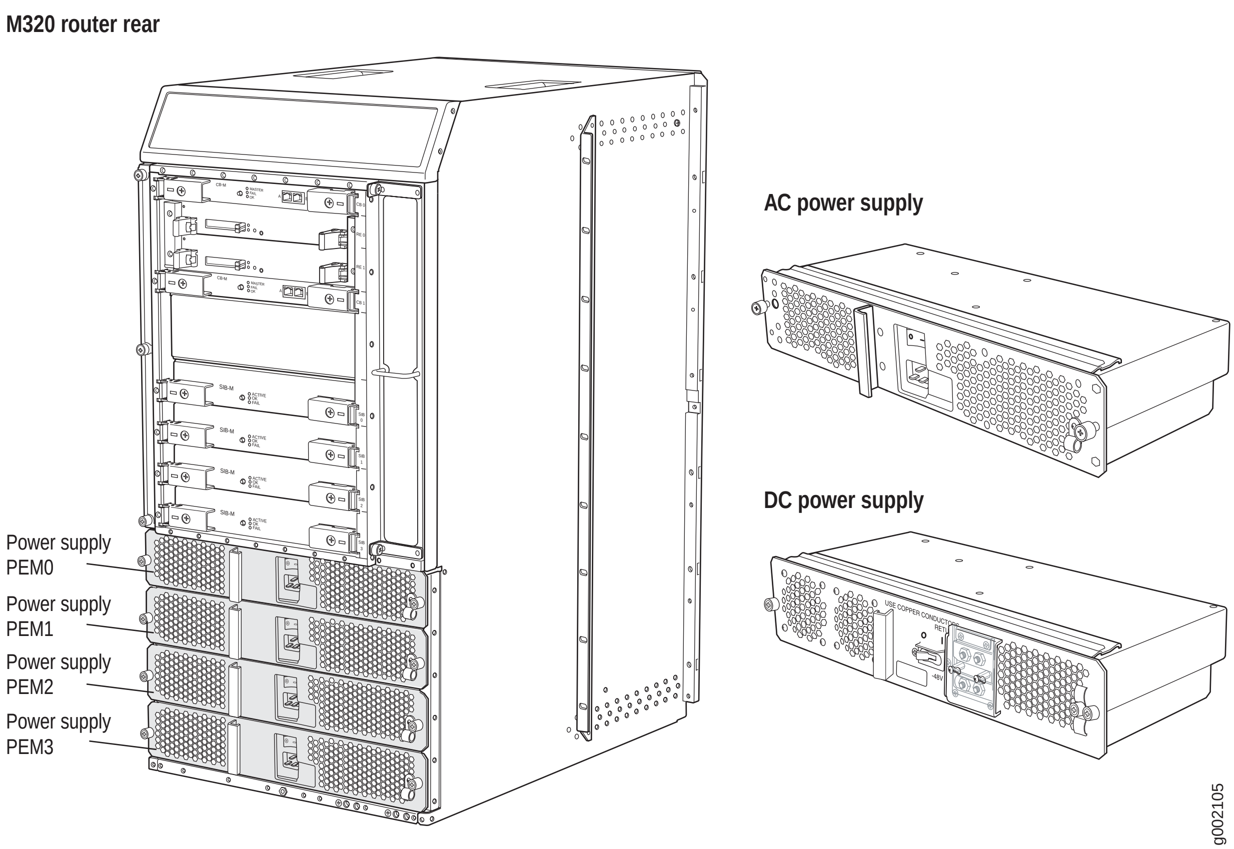
Figure 205: M160 Router Redundant Power Supplies



M320 Router Redundant Power Supplies

The M320 router uses either AC or DC power. Figure 206 shows the M320 router power supplies and where they are installed in the chassis.

Figure 206: M320 Router Redundant Power Supplies



The M320 router supports four power supplies. The AC power supplies are fully redundant. If one power supply fails or is removed, the remaining power supplies instantly assume the entire electrical load. Three power supplies can provide full power for as long as the router is operational.

In the M320 router DC power supply configuration, the router has four DC power supplies, located at the lower rear of the chassis in slots PEM0 through PEM3 (top to bottom). The DC power supplies in slots PEM0 and PEM2 are load-sharing and provide power to the Flexible PIC Concentrators (FPCs) in slots FPC3 through FPC7. The DC power supplies in slots PEM1 and PEM3 are load-sharing and provide power to the FPCs in slots FPC0 through FPC2, Switch Interface Boards (SIBs), Control Boards, and Routing Engines. All DC power supplies provide power to the fan trays.

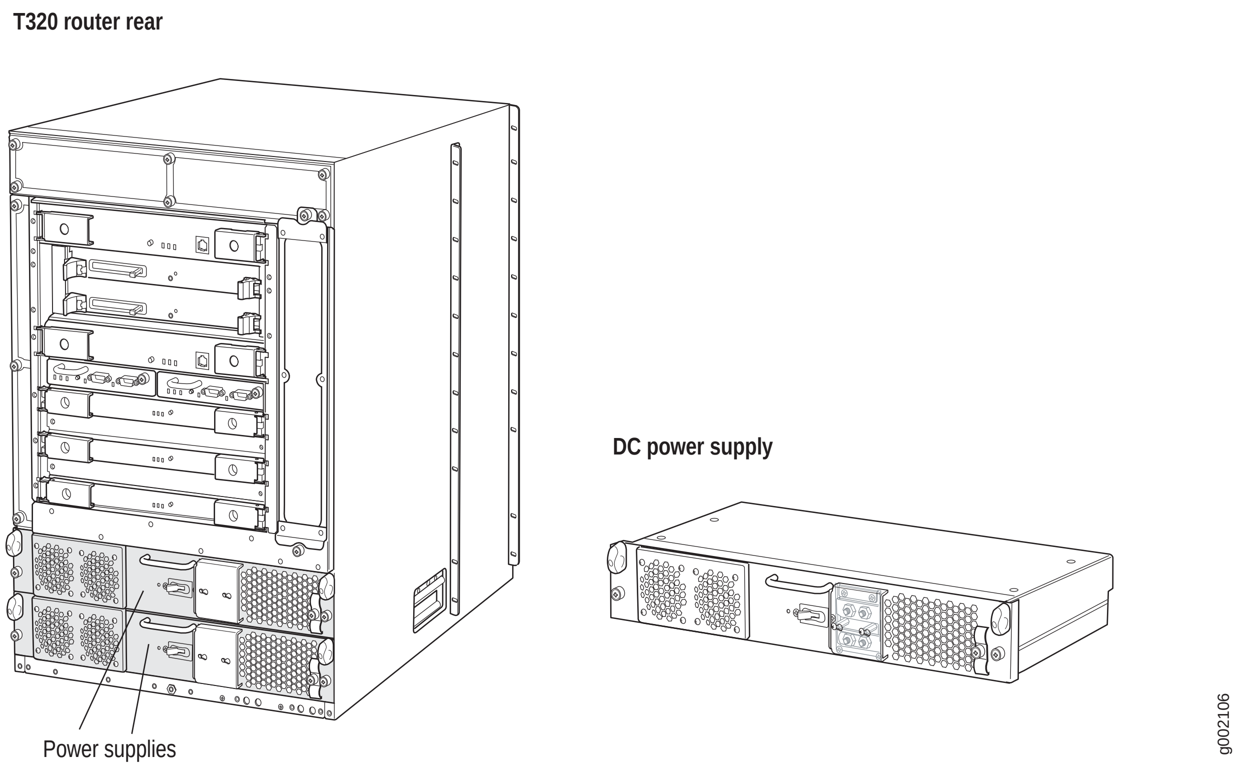
NOTE: The DC power supplies in slots PEM0 and PEM1 must be powered by dedicated power feeds derived from feed A, and the DC power supplies in slots PEM2 and PEM3 must be powered by dedicated power feeds derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated 15 A (250 VAC) circuit breaker.

T320 Router Redundant Power Supplies

Figure 207 shows the T320 router power supplies and where they are installed in the chassis.

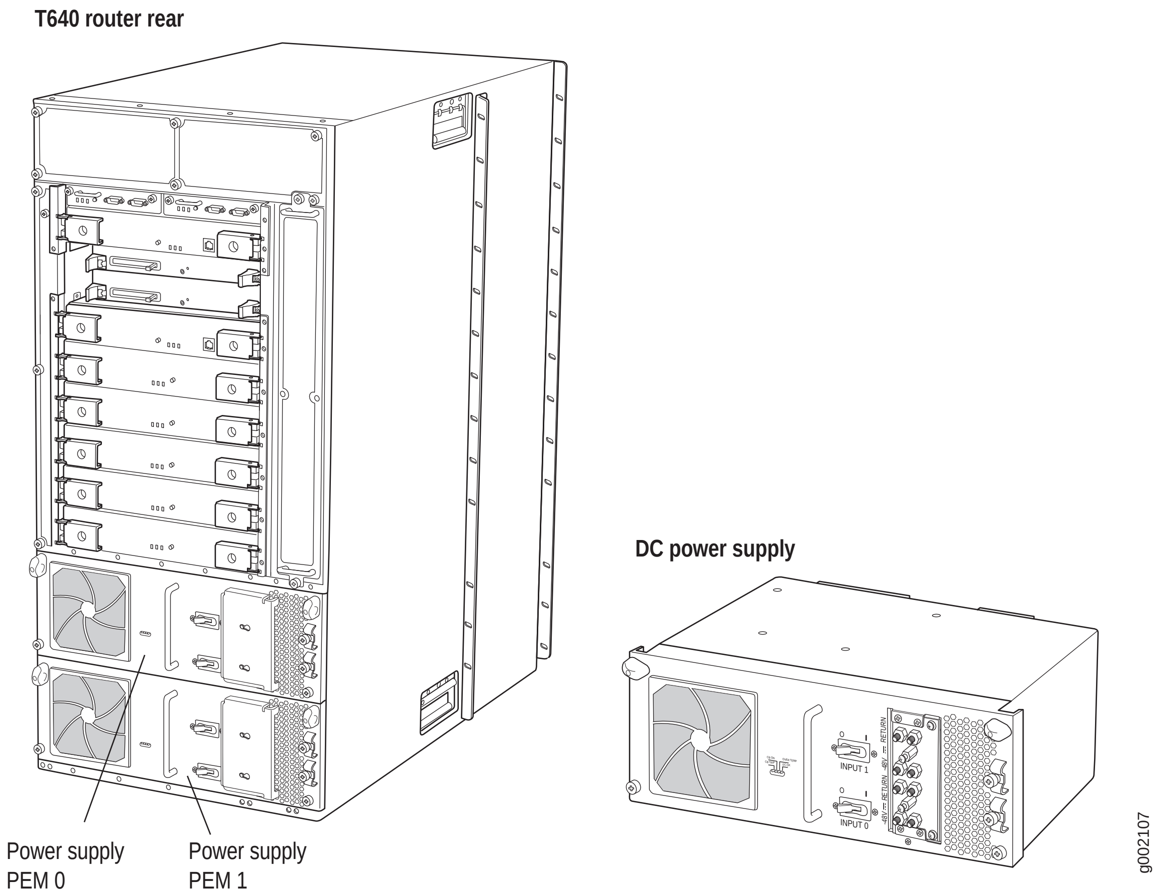
Figure 207: T320 Router Redundant Power Supplies Location



T640 Routing Node Redundant Power Supplies

Figure 208 shows the T640 routing node power supplies and where they are installed in the chassis.

Figure 208: T640 Routing Node Redundant Power Supplies



See Also ■ Monitoring Power Supplies on page 217

Displaying Redundant Power Supplies Installed In The Router

Action To display hardware information about the redundant power supplies installed in a router, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output For M5, M10, M20, M40, and M40e routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                2003              M20
Backplane        REV 07   710-001517   AA7940
Power Supply A   Rev 02   740-001465   000497            AC
Power Supply B   Rev 01   740-001465   000001            AC
```

For M7i routers:

```
user@host> show chassis hardware

user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                19127             M7i
Midplane         REV 02   710-008761   CA0201
Power Supply 1   Rev 04   740-008537   PD10284           AC
[...Output truncated...]
```

For M10i routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                                  M10i
Midplane         REV 02   710-008920   CA0353
Power Supply 0   Rev 04   740-008537   PE18594           AC
Power Supply 1   Rev 04   740-008537   PE18611           AC
Power Supply 2   Rev 04   740-008537   PE18617           AC
Power Supply 3   Rev 04   740-008537   PE18633           AC

[...Output truncated...]
```

For M160 routers:

```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                47                M160
Midplane         REV 02   710-001245   AB4113
FPM CMB          REV 01   710-001642   AA9721
FPM Display      REV 01   710-001647   AA2995
CIP              REV 02   710-001593   AA9886
PEM 0            Rev 01   740-001243   KJ35782           DC
PEM 1            Rev 01   740-001243   kj35756           DC
[...Output truncated...]
```

For M320 routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                19206             M320
Midplane         REV 01   710-009120   RA1277
FPM GBUS         REV 02   710-005928   HL7863
FPM Display      REV 01   710-009351   HP8406
CIP              REV 02   710-005926   BE1813
PEM 0
PEM 1            Rev X1   740-009148   0000005
Routing Engine 0 REV 01   740-008883   212047100102      RE-4.0
Routing Engine 1 REV 01   740-008883   212047100107      RE-4.0
CB 0             REV 01   710-009115   HK0109
CB 1             REV 01   710-009115   HK0110
FPC 0            REV 01   710-008994   HP1418            FPC Type 1
  CPU            REV 01   710-009141   HL7870
  PIC 0          REV 04   750-001894   HE5409            1x G/E, 1000 BASE-SX
  PIC 1          REV 01   750-010240   CB5373            1x G/E SFP, 1000 BASE
    SFP 0        REV 01   740-007326   P11EAW5           SFP-SX
  PIC 3          REV 02   750-002332   AG1661            1x COC12, SMIR
SIB 0            REV 03   750-004762   HL9370            SIB-I-M
SIB 1            REV 03   710-009184   HP8459            SIB-I-M
```

For T320 routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                27714             T320
Midplane         REV 07   710-004339   BF3538
FPM GBUS         REV 04   710-004461   BF5649
FPM Display      REV 04   710-002897   BE9730
CIP              REV 06   710-002895   BF0739
PEM 1            Rev 01   740-004359   NB12576           Power Entry Module
```

For T640 routing nodes:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                55056             T640
Midplane         REV 01   710-005608   BE0888
FPM GBUS         REV 08   710-002901   RA0151
FPM Display      REV 04   710-002897   RA0135
CIP              REV 06   710-002895   HF8317
PEM 0            Rev 06   740-002595   NM17794           Power Entry Module
PEM 1            Rev 04   740-002595   NE15421           Power Entry Module
[...Output truncated...]
```

What It Means For all routers except the M160 router, T320 router, and T640 routing node, the command output displays the power supply slot number, revision level, part number, serial number, and the power supply type.

For the M160 router, T320 router, and the T640 routing node, the command output displays the power supply or Power Entry Module (PEM) slot number, revision level, part number, serial number, and power supply type. When facing the back of the router, PEM0 is located on the right and PEM1 is located on the left.

Checking the Redundant Power Supply Status

Action For more information about monitoring power supplies, see "Checking the Power Supply Status" on page 230.

Checking for Power Supply Alarms

Action For more information about checking for power supply alarms, see "Checking for Power Supply Alarms" on page 235.

Verifying Power Supply Failure

Action For more information about verifying power supply failure, see "Verifying Power Supply Failure" on page 239.

Getting Power Hardware Information

Action For more information about displaying power supply hardware information, see "Getting Power Supply Hardware Information" on page 241.

Replacing a Power Supply

Action For more information about replacing a power supply, see "Replacing a Power Supply" on page 521

Chapter 39

Monitoring Redundant Cooling System Components

You monitor and maintain redundant cooling system components to keep an acceptable operating temperature for the router chassis and its components. (See Table 113.)

Table 113: Checklist for Monitoring Redundant Cooling System Components

Monitor Redundant Cooling System Component Tasks	Command or Action
Understanding Redundant Cooling System Components on page 524	
■ M5 and M10 Router Redundant Cooling System Components on page 525 ■ M7i Router Redundant Cooling System Components on page 526 ■ M10i Router Redundant Cooling System Components on page 527 ■ M20 Router Redundant Cooling System Components on page 527 ■ M40 Router Redundant Cooling System Components on page 529 ■ M40e and M160 Router Redundant Cooling System Components on page 531 ■ M320 Router Redundant Cooling System Components on page 533 ■ T320 Router Redundant Cooling System Components on page 534 ■ T640 Routing Node Redundant Cooling System Components on page 537	
Displaying Redundant Cooling System Components on page 539	show chassis environment
Checking the Redundant Cooling System Status on page 541	See "Checking the Cooling System Status" on page 267.
Checking the Redundant Cooling System Alarms on page 541	See "Checking the Cooling System Alarms" on page 269 and "Display the Current Router Alarms" on page 61.
Removing a Cooling System Component on page 541	See "Replacing a Cooling System Component" on page 273.
Returning Redundant Cooling System Components on page 541	See "Return the Failed Component" on page 86, or follow the procedure in appropriate router hardware guide.

Understanding Redundant Cooling System Components

Purpose Inspect the router redundant cooling system components to ensure that air is flowing through the router to cool the components installed in the router chassis. If the router temperature exceeds a critical level, the router automatically shuts down.

What Are Redundant Cooling System Components Redundant cooling system components are more than just one fan or impeller installed in a router to ensure that the air is flowing through the router and that an acceptable temperature is maintained to cool the components installed in the chassis.

Table 114 describes the redundant cooling system components and characteristics for each routing platform.

Table 114: Redundant Cooling System Components Characteristics Per Routing Platform

Cooling System Component	M5 and M10	M7i	M10i	M20	M40	M40e	M160	M320/T320/T640
Fan tray	1 fan tray with 4 fans	1	2	3 front 1 rear		1	1 lower	2 front 1 rear
Power supply integrated fan	_	_	_	2	2	_	Cooled by air flowing through the chassis	Cooled by air flowing through the chassis
Impellers	_	_	_	_	2 pairs	1 central 1 rear upper 1 rear lower	1 upper 2 rear	_
Fan assemblies	_	_	_	_	3	_	_	_
Air filter	_	_	_	_	1	1	1	1 front 1 rear

The following sections describe the various routing platform cooling systems:

- M5 and M10 Router Redundant Cooling System Components on page 525
- M7i Router Redundant Cooling System Components on page 526
- M10i Router Redundant Cooling System Components on page 527
- M20 Router Redundant Cooling System Components on page 527
- M40 Router Redundant Cooling System Components on page 529
- M40e and M160 Router Redundant Cooling System Components on page 531
- M320 Router Redundant Cooling System Components on page 533
- T320 Router Redundant Cooling System Components on page 534
- T640 Routing Node Redundant Cooling System Components on page 537

M5 and M10 Router Redundant Cooling System Components

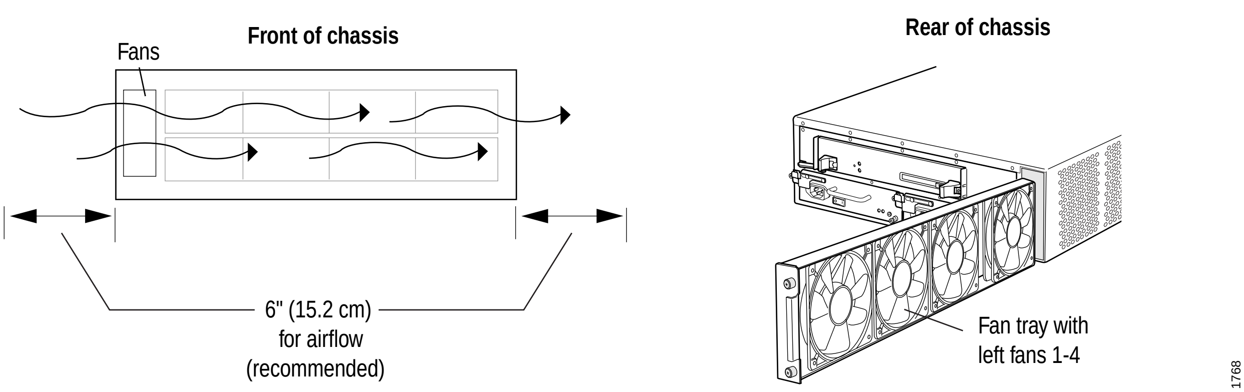
The M5 and M10 router cooling system consists of a fan tray containing four fans that inserts into the left side of the chassis (left fans 1 through 4). The fan tray connects to the router midplane and provides side-to-side cooling. (See Figure 209.)

The fan tray is hot-removable and hot-insertable. You can remove and replace these components without powering down the system and disrupting routing functions.

The cooling system is fault-tolerant. The router can tolerate the failure of a single fan for approximately 36 hours. If a fan fails, the router issues a yellow alarm and the yellow alarm LED on the craft interface lights. If the router temperature exceeds the critical level, the router automatically shuts down.

CAUTION: Do not operate the router for more than 1 minute without a fan tray.

Figure 209: M5 and M10 Router Cooling System and Airflow



M7i Router Redundant Cooling System Components

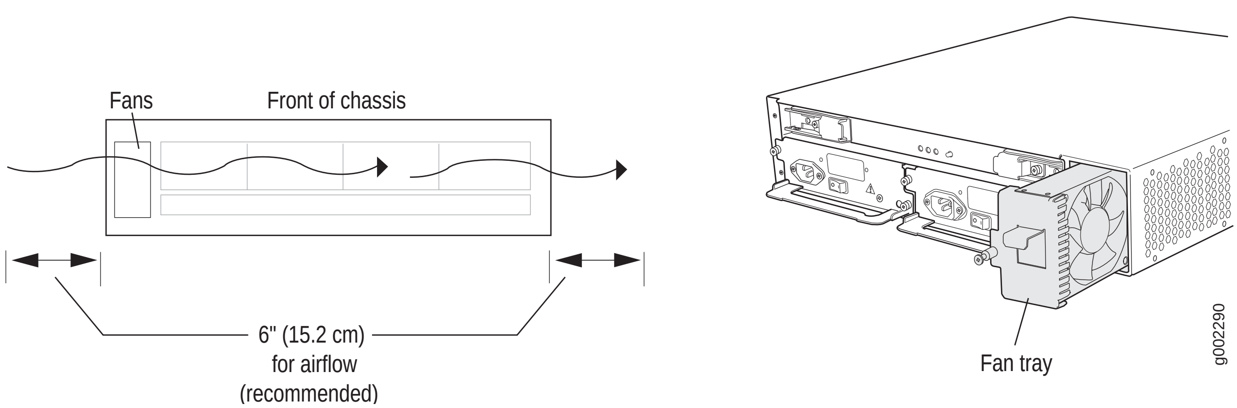
The M7i router cooling system consists of a fan tray containing four individually fault-tolerant fans. The fan tray inserts into the left side of the chassis (left fans 1 through 4) and connects directly to the router midplane. If a single fan fails, the remaining fans continue to function indefinitely. The fan tray provides side-to-side cooling. (See Figure 210.)

The fan tray is hot-removable and hot-insertable. You can remove and replace these components without powering down the system and disrupting routing functions.

The cooling system is fault-tolerant. The router can tolerate the failure of a single fan for approximately 36 hours. If a fan fails, the router issues a yellow alarm and the yellow alarm LED on the craft interface lights. If the router temperature exceeds the critical level, the router automatically shuts down.

CAUTION: Do not operate the router for more than 1 minute without a fan tray.

Figure 210: M7i Router Cooling System and Airflow

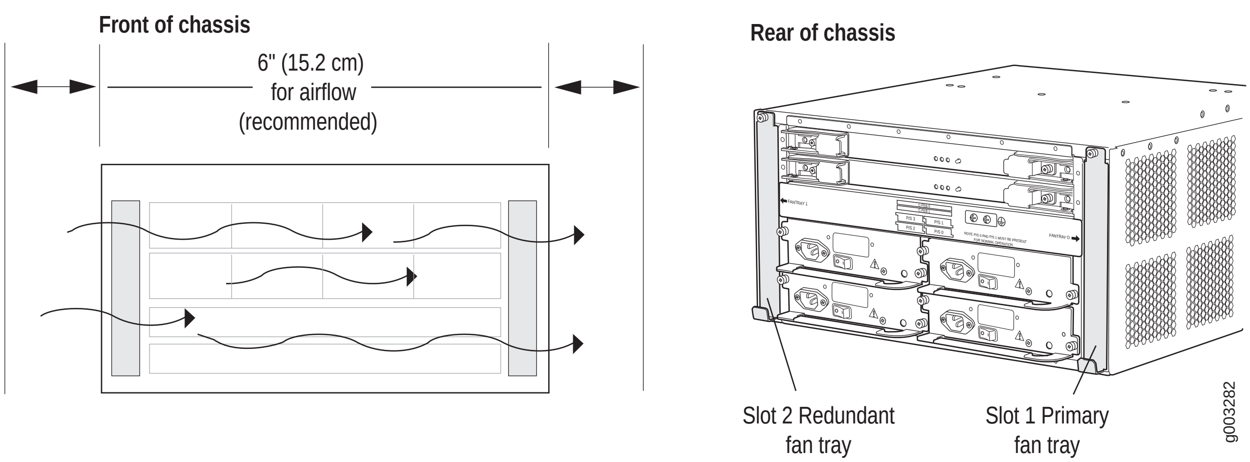


M10i Router Redundant Cooling System Components

The M10i router cooling system consists of two fan trays, located along the left and right side of the chassis, that provide side-to-side cooling (see Figure 211). They connect directly to the router midplane. Each fan tray is a single unit containing eight individually fault-tolerant fans. If a single fan fails, the remaining fans continue to function indefinitely. For proper airflow, the primary fan tray should be installed in slot `1` (the left slot looking at the chassis from the rear) and must be installed for proper cooling at all times. The redundant fan tray, if present, should be installed in slot `0` on the right. This fan tray provides additional cooling and redundancy. The fan tray is hot-removable and hot-insertable.

CAUTION: Do not remove both fan trays for more than one minute while the router is operating. The fans are the sole source of cooling, and the router will overheat when they are absent.

Figure 211: M10i Router Cooling System Components and Airflow



M20 Router Redundant Cooling System Components

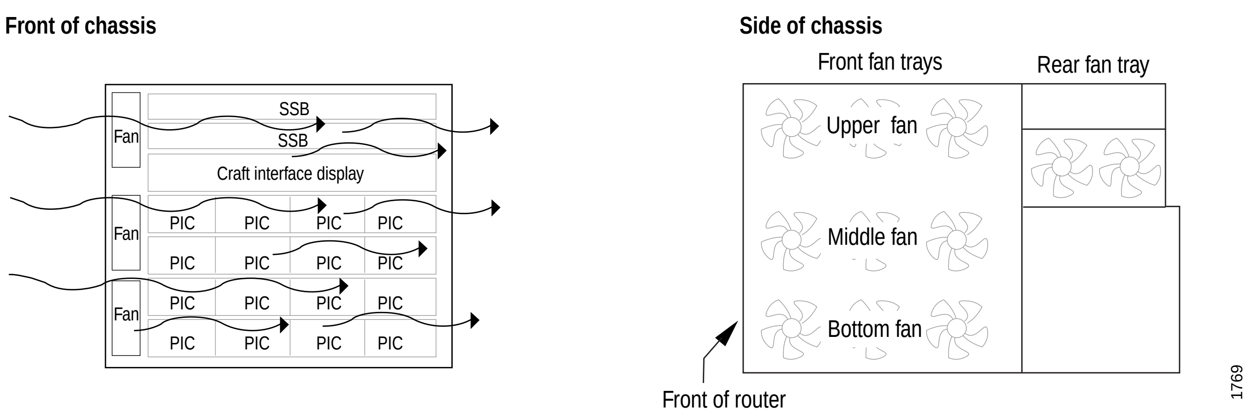
The M20 router cooling system includes:

- Three front fan trays—Cool the Flexible PIC Concentrators (FPCs) and the System and Switch Board (SSB). These fan trays are located on the left front side of the chassis.
- One rear fan tray—Cools the Routing Engine. This fan tray is located immediately to the right of the Routing Engine.
- Power supply integrated fan—A built-in fan cools each power supply.

The four fan trays plug directly into the router midplane and work together to provide side-by-side cooling.

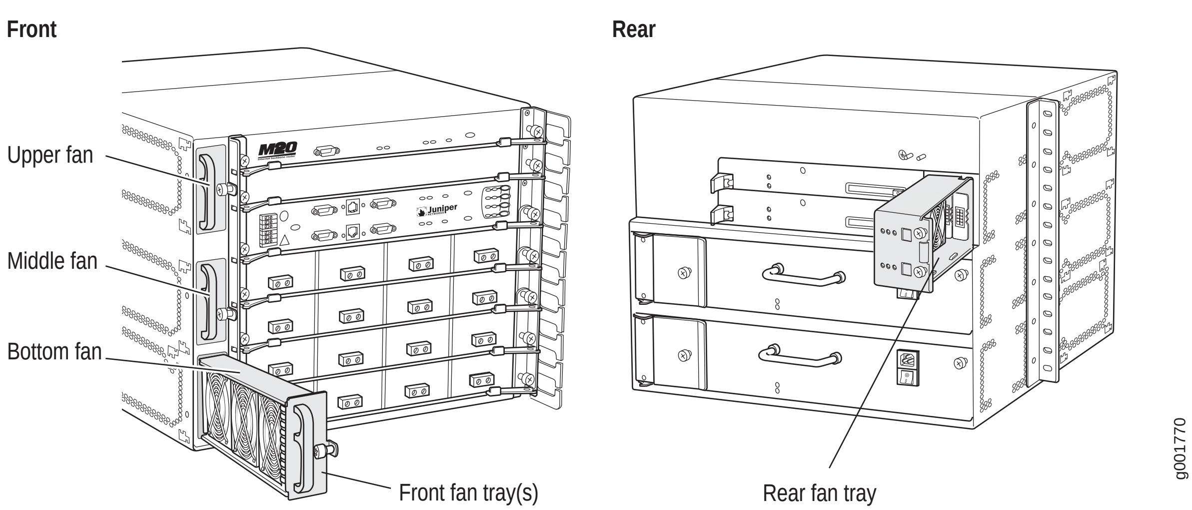
The fans operate in unison to maintain an acceptable operating temperature for the Routing Engine and midplane. Each cooling subsystem maintains a separate airflow, and each is monitored independently for temperature control. Figure 212 shows the M20 router cooling system components and airflow.

Figure 212: M20 Router Cooling System and Airflow



Both front and rear fan trays are hot-removable and hot-insertable. You can remove and replace these components without powering down the system and disrupting routing functions. Figure 213 shows the M20 router cooling system components.

Figure 213: M20 Router Cooling System Components



M40 Router Redundant Cooling System Components

The M40 router cooling system consists of three separate subsystems (see Figure 214):

- Impellers—Two redundant pairs of impellers (top impeller and bottom impeller) cool the Packet Forwarding Engine components (backplane, System Control Board [SCB], FPCs, and Physical Interface Cards [PICs]). During normal operation, both pairs of impellers function at less than full capacity.
- Triple fan assemblies—Three load-sharing fans cool the backplane and the Routing Engine (rear left fan, rear center fan, and rear right fan).
- Power supply integrated fan—A built-in fan cools each power supply.

Each cooling subsystem maintains a separate airflow, and each is monitored independently for temperature control. Figure 214 shows the M40 router cooling system airflow.

Temperature sensors on the backplane, the SCB, and the FPCs control the speed of the impellers. Impeller failure triggers the red alarm LED on the craft interface. If the temperature passes a certain threshold, the JUNOS software turns off the power supplies.

The M40 router is designed to run normally with all three fans sharing the load equally and running at half speed.

Figure 214: M40 Router Cooling System and Airflow

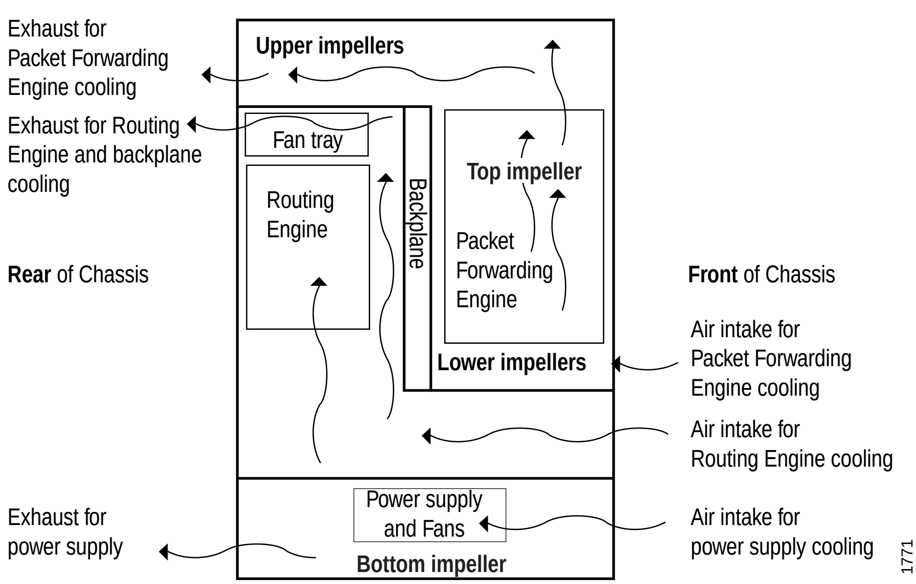


Figure 215 shows the M40 router cooling system impeller trays.

Figure 215: M40 Router Impeller Trays

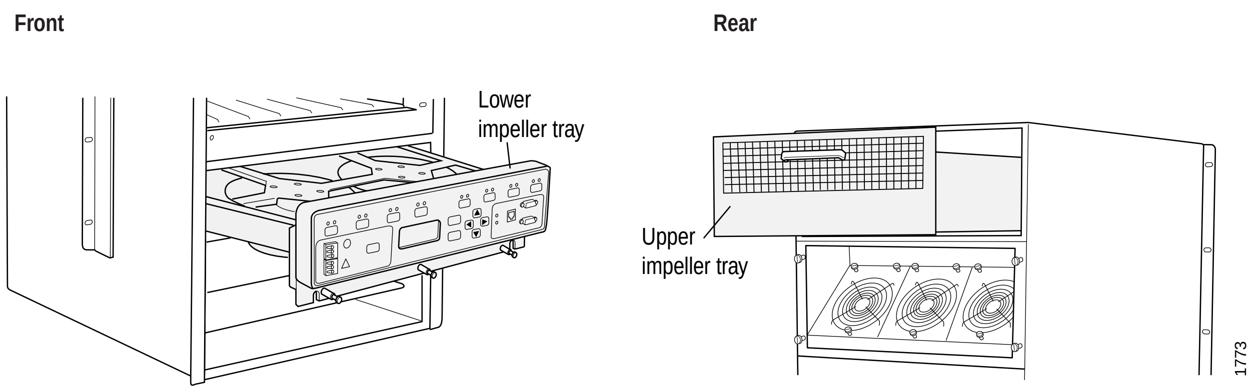
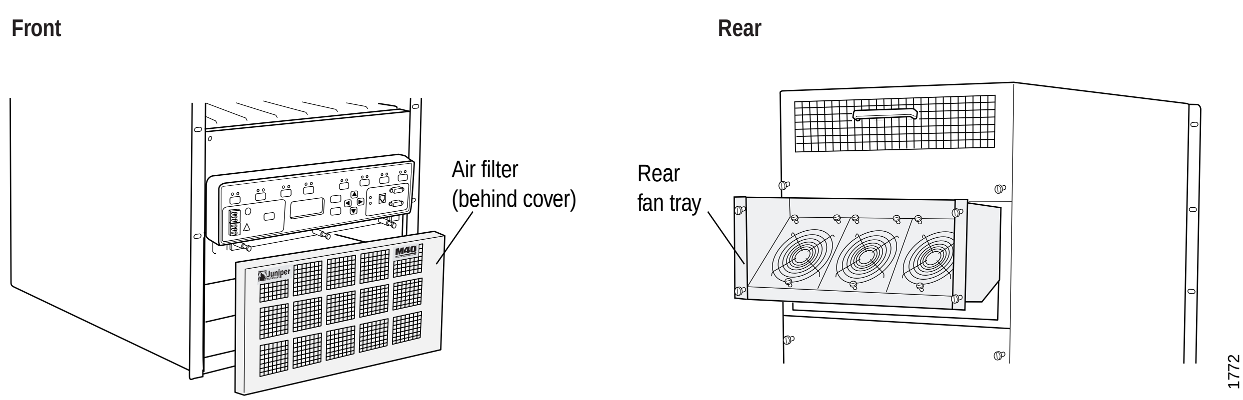


Figure 216 shows the M40 router air filter and fan tray.

Figure 216: M40 Router Air Filter and Fan Tray



M40e and M160 Router Redundant Cooling System Components

The M40e and M160 routers include the following cooling system components:

- Front cooling subsystem—Cools the FPCs, PICs, and midplane. It includes a fan tray located behind the cable management system and a large, central impeller behind the craft interface (fan tray front left, fan tray front right, fan tray rear left, fan tray rear right, and front top blower).
- Rear cooling subsystem—Cools the Switching and Forwarding Modules (SFMs), host module, PFE Clock Generators (PCGs), and power supplies. It includes one impeller located at the upper right of the chassis rear and another at the lower left, as shown in Figure 217 (rear top blower and rear bottom blower). The upper and lower impellers are not interchangeable.

Figure 217 shows the M40e and M160 router cooling system components and airflow.

Figure 217: M40e and M160 Router Cooling System and Airflow

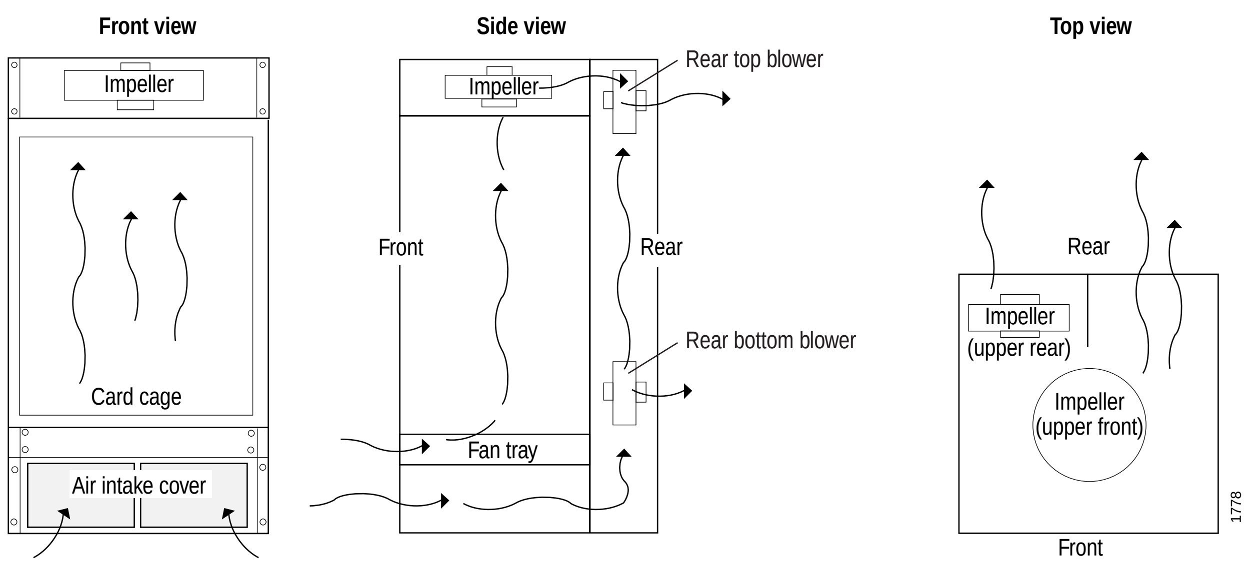
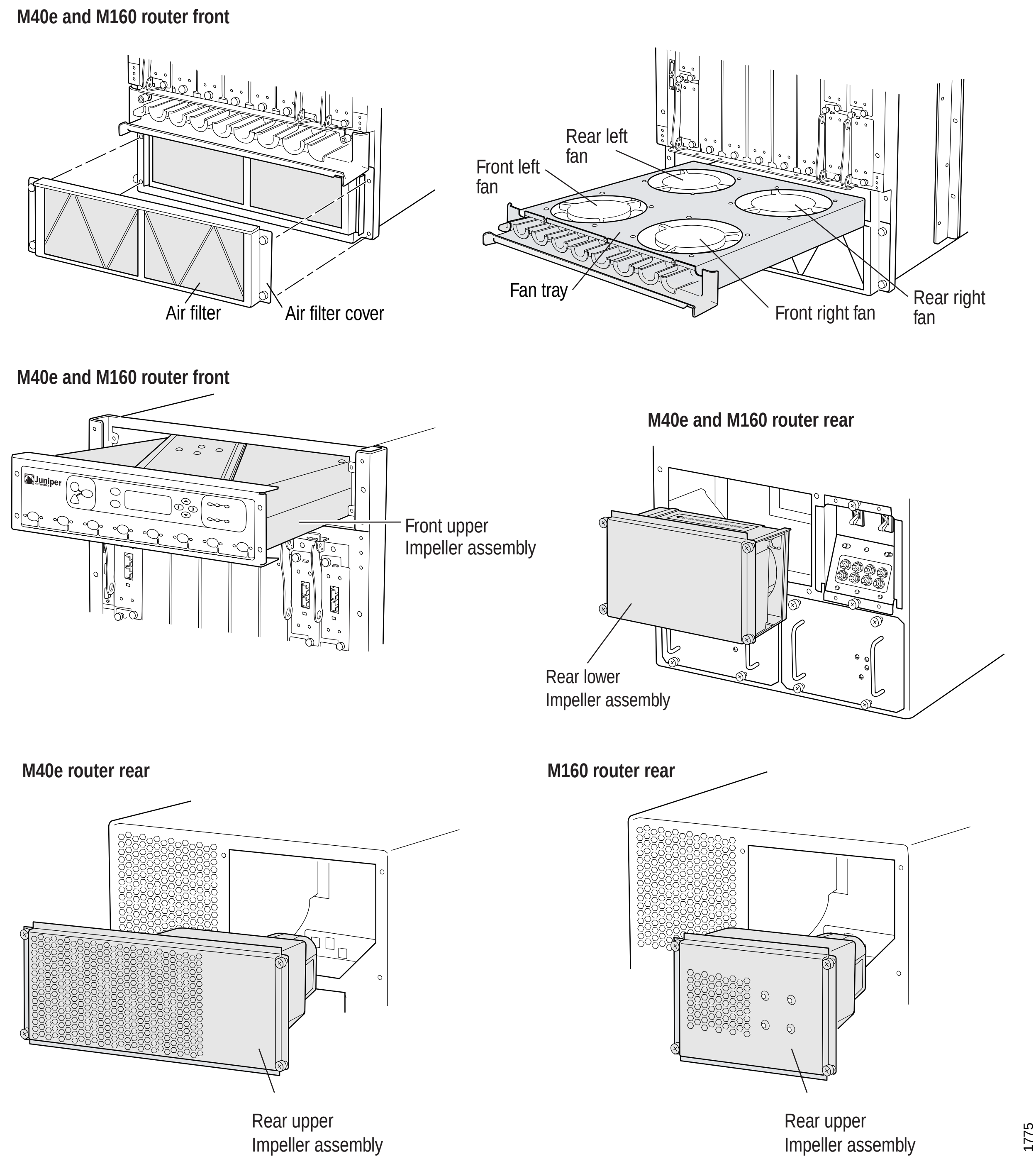


Figure 218 shows the M40e and M160 router cooling system components.

Figure 218: M40e and M160 Router Cooling System Components



See Also ■ Monitoring Power Supplies on page 217

M320 Router Redundant Cooling System Components

The M320 router includes the following cooling system components:

- Two front fan trays
- Front air filter
- Rear fan tray
- Rear air filter

The cooling system components work together to keep all router components within the acceptable temperature range. All fan trays and filters are hot-insertable and hot-removable. The two front fan trays are interchangeable. The front and rear fan trays are not interchangeable.

Figure 219 shows the M320 router cooling system airflow.

Figure 219: M320 Router Cooling System and Airflow

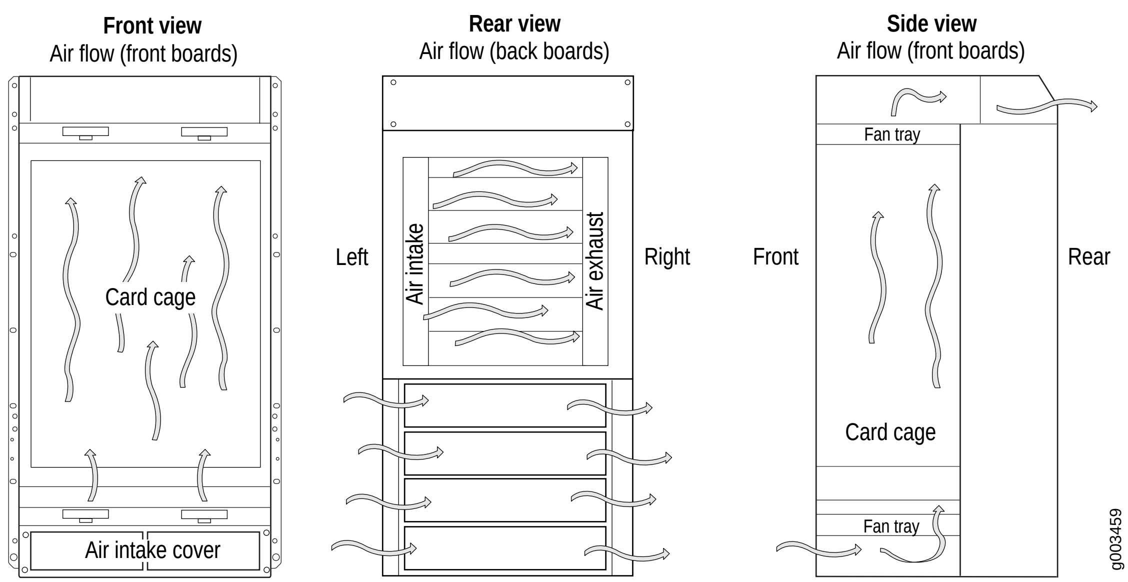
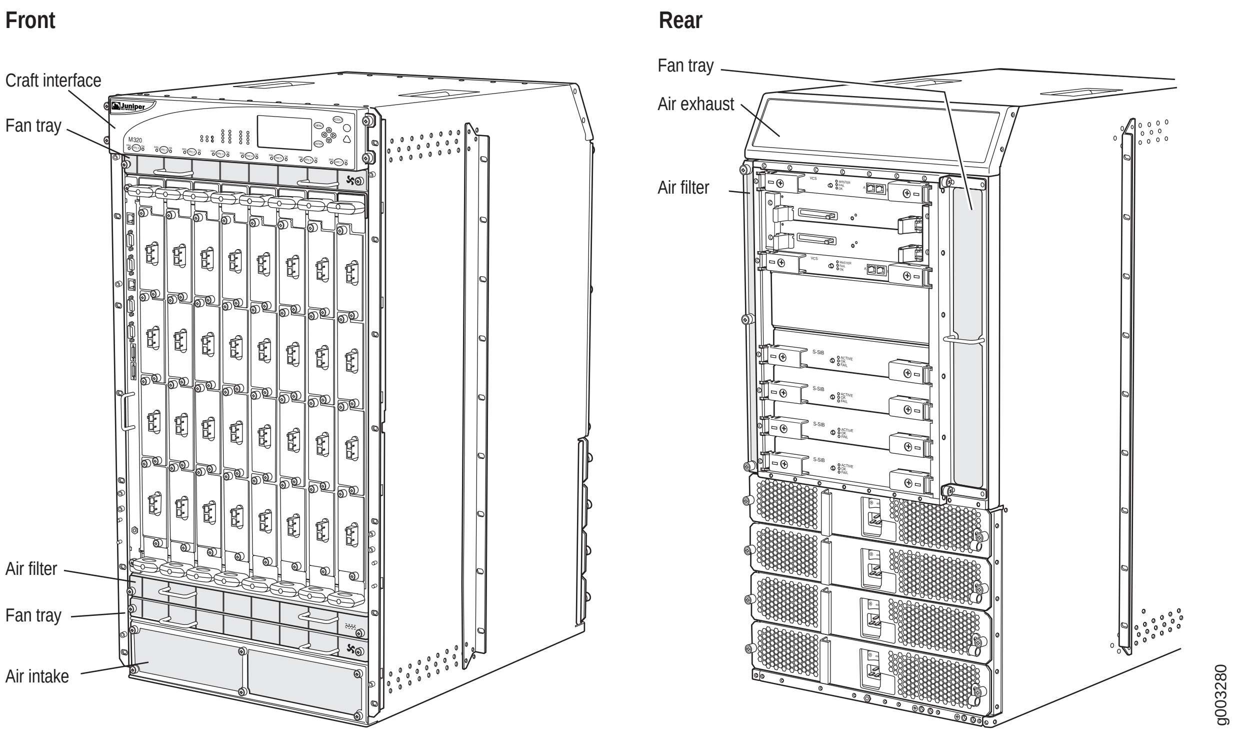


Figure 220 shows the M320 router cooling system components.

Figure 220: M320 Router Cooling System Components



The host subsystem monitors the temperature of the router components. When the router is operating normally, the fans function at lower than full speed. If a fan fails or the ambient temperature rises above a threshold, the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range. If the ambient maximum temperature specification is exceeded and the system cannot be adequately cooled, the Routing Engine shuts down some or all of the hardware components.

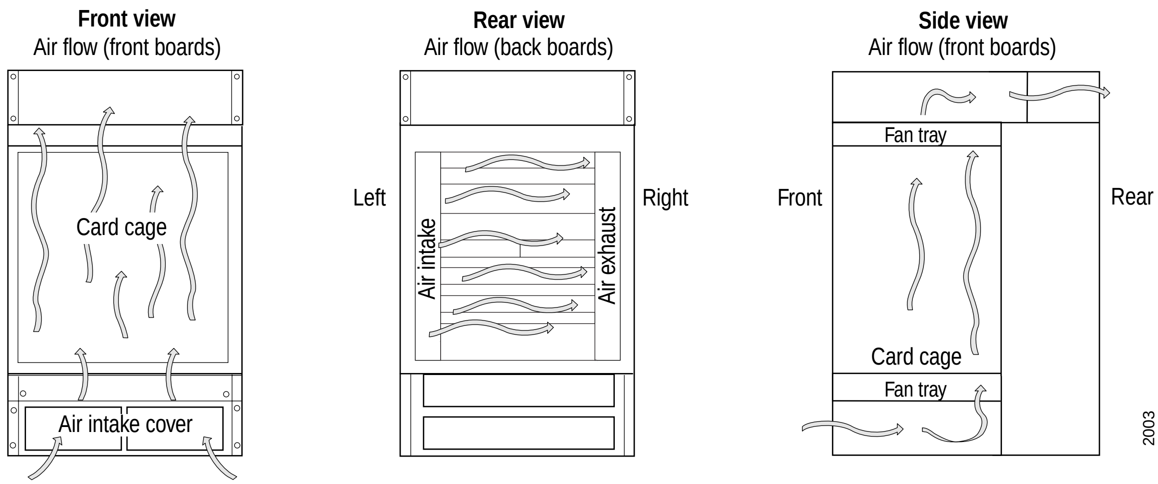
T320 Router Redundant Cooling System Components

The T320 router cooling system includes:

- Two front fan trays
- Front air filter
- Rear fan tray
- Rear air filter

The cooling system components work together to keep all router components within the acceptable temperature range (see Figure 221 on page 535). All fan trays and filters are hot-insertable and hot-removable. The two front fan trays are interchangeable. The front and rear fan trays are not interchangeable.

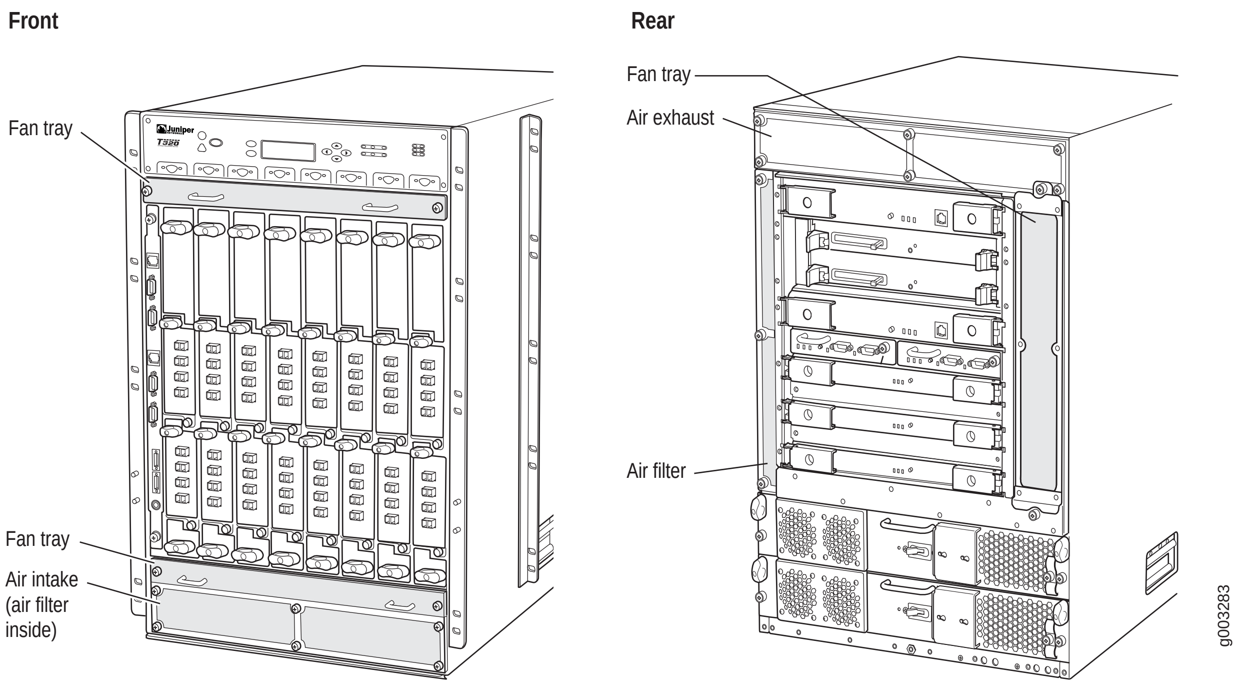
Figure 221: T320 Router Cooling System and Airflow



The cooling system has redundant components, which are controlled by the host subsystem. If one of the fans fails, the host subsystem increases the speed of the remaining fans to provide sufficient cooling for the router indefinitely.

The host subsystem monitors the temperature of the router components. When the router is operating normally, the fans function at lower than full speed. If a fan fails, the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range. Cooling system components can be removed and replaced without powering down or disconnecting power to the router. Figure 222 shows the T320 router cooling system components.

Figure 222: T320 Router Cooling System Components



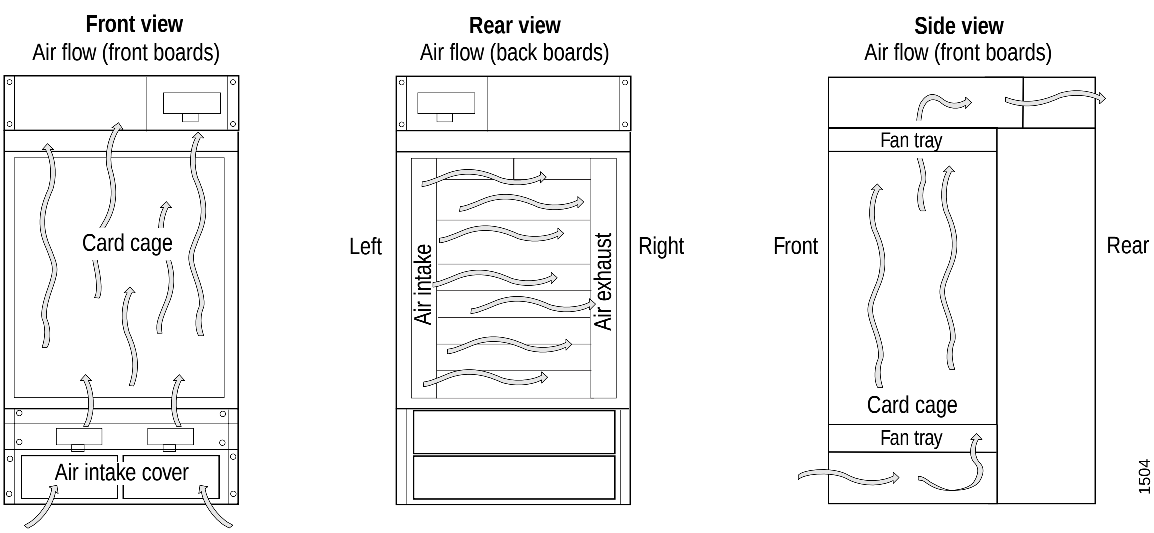
T640 Routing Node Redundant Cooling System Components

The T640 routing node cooling system includes:

- Two front fan trays
- Front air filter
- Rear fan tray
- Rear air filter

The cooling system components work together to keep all router components within the acceptable temperature range (see Figure 223). All fan trays and filters are hot-insertable and hot-removable. The two front fan trays are interchangeable. The front and rear fan trays are not interchangeable.

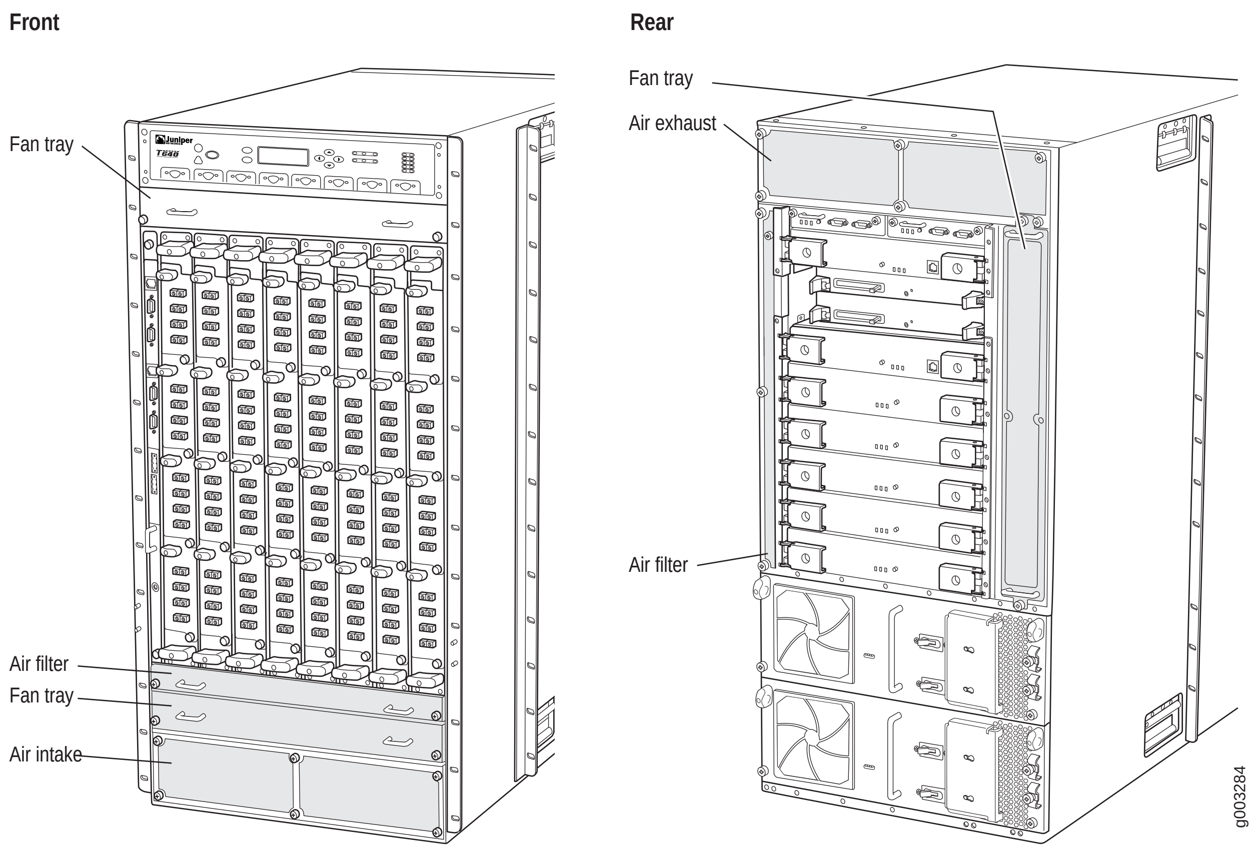
Figure 223: T640 Routing Node Cooling System and Airflow



The cooling system has redundant components, which are controlled by the host subsystem. If one of the fans fails, the host subsystem increases the speed of the remaining fans to provide sufficient cooling for the router indefinitely.

The host subsystem monitors the temperature of the router components. When the router is operating normally, the fans function at lower than full speed. If a fan fails, the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range. Cooling system components can be removed and replaced without powering down or disconnecting power to the router. Figure 224 on page 538 shows the T640 routing node cooling system components.

Figure 224: T640 Routing Node Cooling System Components



Displaying Redundant Cooling System Components

Action To display the redundant cooling system components that are installed in a routing platform, use the following command-line interface (CLI) command:

user@host> **show chassis environment**

Sample Output For M5 and M10 routers (see also Figure 209 on page 525):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Left Fan 1            OK         Spinning at normal speed
      Left Fan 2            OK         Spinning at normal speed
      Left Fan 3            OK         Spinning at normal speed
      Left Fan 4            OK         Spinning at normal speed
Misc  Craft Interface       OK
```

For an M7i router (see also Figure 210 on page 526):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Fan 1                 OK         Spinning at normal speed
      Fan 2                 OK         Spinning at normal speed
      Fan 3                 OK         Spinning at normal speed
      Fan 4                 OK         Spinning at normal speed
```

For an M10i router (see also Figure 211 on page 527):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Fan Tray 0 Fan 1      OK         Spinning at normal speed
      Fan Tray 0 Fan 2      OK         Spinning at normal speed
      Fan Tray 0 Fan 3      OK         Spinning at normal speed
      Fan Tray 0 Fan 4      OK         Spinning at normal speed
      Fan Tray 0 Fan 5      OK         Spinning at normal speed
      Fan Tray 0 Fan 6      OK         Spinning at normal speed
      Fan Tray 0 Fan 7      OK         Spinning at normal speed
      Fan Tray 0 Fan 8      OK         Spinning at normal speed
      Fan Tray 1 Fan 1      OK         Spinning at normal speed
      Fan Tray 1 Fan 2      OK         Spinning at normal speed
      Fan Tray 1 Fan 3      OK         Spinning at normal speed
      Fan Tray 1 Fan 4      OK         Spinning at normal speed
      Fan Tray 1 Fan 5      OK         Spinning at normal speed
      Fan Tray 1 Fan 6      OK         Spinning at normal speed
      Fan Tray 1 Fan 7      OK         Spinning at normal speed
      Fan Tray 1 Fan 8      OK         Spinning at normal speed
```

For an M20 router (see also Figure 212 on page 528):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Rear Fan              OK         Spinning at normal speed
      Front Upper Fan       OK         Spinning at normal speed
      Front Middle Fan      OK         Spinning at normal speed
      Front Bottom Fan      OK         Spinning at normal speed
Misc  Craft Interface       OK
```

For an M40 router (see also Figure 214 on page 529):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Top Impeller          OK         Spinning at normal speed
      Bottom impeller       OK         Spinning at normal speed
      Rear Left Fan         OK         Spinning at normal speed
      Rear Center Fan       OK         Spinning at normal speed
      Rear Right Fan        OK         Spinning at normal speed
Misc  Craft Interface       OK
```

For M40e and M160 routers (see also Figure 217 on page 531):

```
user@host> show chassis environment
Class Item                  Status     Measurement
[...Output truncated...]
Fans  Rear Bottom Blower    OK         Spinning at normal speed
      Rear Top Blower       OK         Spinning at normal speed
      Front Top Blower      OK         Spinning at normal speed
      Fan Tray Rear Left    OK         Spinning at normal speed
      Fan Tray Rear Right   OK         Spinning at normal speed
      Fan Tray Front Left   OK         Spinning at normal speed
      Fan Tray Front Right  OK         Spinning at normal speed
Misc  CIP                   OK
```

For an M320 router (see also Figure 219 on page 533):

```
user@host> show chassis environment
Class Item                  Status     Measurement
Fan   Top Left Front fan    OK         Spinning at normal speed
      Top Right Rear fan    OK         Spinning at normal speed
      Top Right Front fan   OK         Spinning at normal speed
      Top Left Rear fan     OK         Spinning at normal speed
      Bottom Left Front fan  OK        Spinning at normal speed
      Bottom Right Rear fan  OK        Spinning at normal speed
      Bottom Right Front fan OK        Spinning at normal speed
      Bottom Left Rear fan  OK         Spinning at normal speed
      Rear Fan 1 (TOP)      OK         Spinning at normal speed
      Rear Fan 2            OK         Spinning at normal speed
      Rear Fan 3            OK         Spinning at normal speed
      Rear Fan 4            OK         Spinning at normal speed
      Rear Fan 5            OK         Spinning at normal speed
      Rear Fan 6            OK         Spinning at normal speed
      Rear Fan 7 (Bottom)   OK         Spinning at normal speed
```

For T320 routers and T640 routing nodes (see also Figure 221 on page 535, Figure 222 on page 536, Figure 223 on page 537, and Figure 224 on page 538):

```
user@host> show chassis environment
Class Item                  Status     Measurement
Fans  Top Left Front fan    OK         Spinning at normal speed
      Top Left Middle fan   OK         Spinning at normal speed
      Top Left Rear fan     OK         Spinning at normal speed
      Top Right Front fan   OK         Spinning at normal speed
      Top Right Middle fan  OK         Spinning at normal speed
      Top Right Rear fan    OK         Spinning at normal speed
      Bottom Left Front fan  OK        Spinning at normal speed
      Bottom Left Middle fan OK        Spinning at normal speed
      Bottom Left Rear fan  OK         Spinning at normal speed
      Bottom Right Front fan OK        Spinning at normal speed
```

```
Bottom Right Middle fan OK        Spinning at normal speed
Bottom Right Rear fan  OK         Spinning at normal speed
Fourth Blower from top OK         Spinning at normal speed
Bottom Blower          OK         Spinning at normal speed
Middle Blower          OK         Spinning at normal speed
Top Blower             OK         Spinning at normal speed
Second Blower from top OK         Spinning at normal speed
```

What It Means The command output shows the fans, impellers, or blowers monitored for the router type. The command output displays the fan, impeller, or blower status and the spinning speed. The status can be OK, Testing (during initial power-on), Failed, or Absent. Measurement indicates if the fan or impeller is spinning at normal or high speed.

Checking the Redundant Cooling System Status

Action For more information about checking the status of cooling system components, see “Checking the Cooling System Status” on page 267.

Checking the Redundant Cooling System Alarms

Action For more information about checking the cooling system alarms, see “Checking the Cooling System Alarms” on page 269. For more information about conditions that trigger cooling system alarms, see “Display the Current Router Alarms” on page 61.

Removing a Cooling System Component

For more information about removing or swap testing cooling system components, see “Replacing a Cooling System Component” on page 273.

Returning Redundant Cooling System Components

Action To return a cooling system component, see “Return the Failed Component” on page 86 or the appropriate router hardware guide.

Chapter 40
Monitoring Redundant SIBs

You monitor and maintain redundant Switch Interface Boards (SIBs) installed in the M320 and T320 routers and the T640 Internet routing node to ensure that there is no interruption of switching function to the destination Flexible PIC Concentrator (FPC). The SIBs create the switch fabric, providing up to a total of 640 million packets per second (Mpps) of forwarding.

Table 115 provides a checklist of tasks for you to perform to monitor redundant SIBs.

Table 115: Checklist for Monitoring Redundant SIBs

Monitor Redundant SIB Tasks	Command or Action
Understanding Redundant SIBs on page 544 ■ M320 Router SIBs on page 546 ■ T320 Router SIBs on page 546 ■ T640 Routing Node SIBs on page 546	
Displaying Redundant SIB Hardware Information on page 547	show chassis hardware
Displaying SIB Redundancy Information on page 547	show chassis sib show chassis environment sib
Monitoring Redundant SIB Status on page 548	See "Monitoring the SIB Status" on page 329.
Displaying SIB Alarms on page 548	See "Monitoring the SIB Status" on page 329
Performing a Swap Test on a SIB on page 549	See "Verifying SIB Failure" on page 334.
Returning the SIB on page 549	Locate the serial number label on the left side of the SIB top panel, and follow the procedure "Return the Failed Component" on page 86. Or follow the procedure in the appropriate router hardware guide.

Understanding Redundant SIBs

Purpose Inspect redundant SIBs to ensure that they provide the switching function to the destination FPCs.

What Are Redundant SIBs Redundant SIBs are multiple SIBs that are installed in the M320 router, T320 router, and the T640 routing node. In the event of a failure, one of the SIBs acts as backup for the failed SIB. For more information, see "SIB Location and Redundancy" on page 545.

Table 116 shows the SIB characteristics for the M320 router, T320 router, and the T640 routing node.

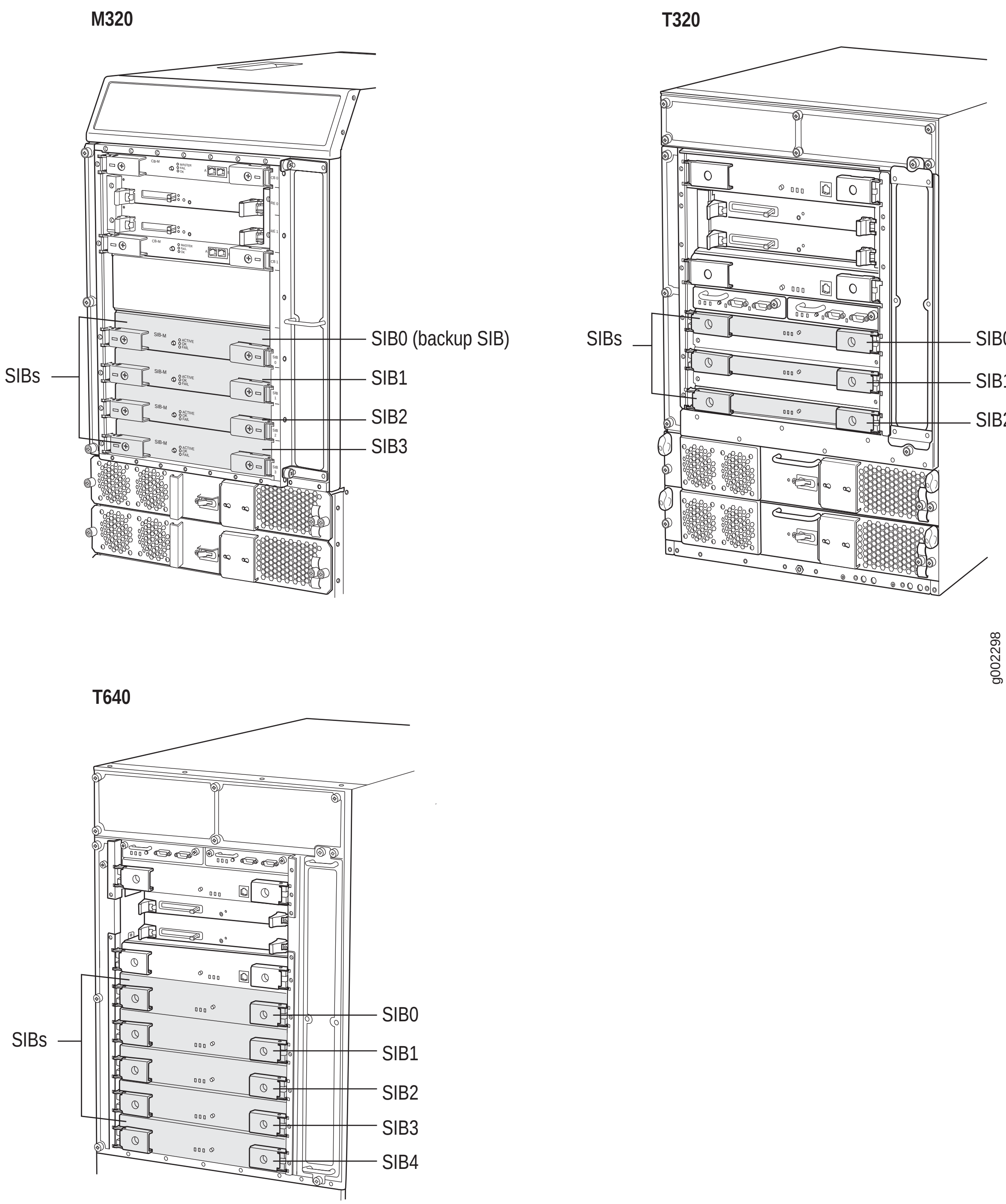
Table 116: SIB Packet Forwarding Characteristics

Routing Platform	Million Packets per Second (Mpps) Forwarding	Number of SIBs per Chassis	Redundancy
M320	385	4	No
T320	320	3	Yes
T640	640	5	Yes

SIB Location and Redundancy

Figure 225 shows the location of the SIBs in the M320 router, T320 router, and T640 routing node.

Figure 225: M320 Router, T320 Router, and T640 Routing Node SIB Location



The following sections describe SIB redundancy on various routing platforms:

- M320 Router SIBs on page 546
- T320 Router SIBs on page 546
- T640 Routing Node SIBs on page 546

M320 Router SIBs

Four SIBs are installed in the M320 router. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB3 (top to bottom). (See Figure 225 on page 545.) All four SIBs are active, and there is no backup.

T320 Router SIBs

Three SIBs are installed in the router. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB2. (See Figure 225 on page 545.)

Each FPC has a dedicated ASIC with five high-speed links that connect to the SIBs. Two high-speed links connect to SIB1 and SIB2. One high-speed link connects to SIB0. SIB0 acts as a backup to SIB1 and SIB2. In the event of a complete SIB failure, SIB0 will become active. Because SIB0 has only one high-speed link to each FPC, only three links will remain active. A slight degradation in forwarding capacity may occur. When the failed SIB is replaced, it will become active and SIB0 will revert to backup. The router will regain full forwarding capacity.

T640 Routing Node SIBs

Five SIBs are installed in the routing node. The SIBs are located at the center rear of the chassis in the slots labeled SIB0 through SIB4 (top to bottom). (See Figure 225 on page 545.)

Each FPC1 and FPC2 has a dedicated ASIC with five high-speed links that connect to the SIBs (one link per SIB). An FPC3 has two dedicated ASICs, and each ASIC has five high-speed links that connect to the SIBs (a total of 10 links). One of the five SIBs—usually SIB4—acts as a backup to the remaining four SIBs. In the event of a SIB failure, the backup SIB becomes active and traffic forwarding continues without any degradation. When the failed SIB is replaced, it becomes the new backup.

The SIBs are hot-insertable and hot-removable.

See Also

- Monitoring the Host Subsystem on page 289
- Monitoring the SIBs on page 325

Displaying Redundant SIB Hardware Information

Action To display the redundant SIB hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                20079             M160
[...Output truncated...]
SIB 0            REV 05   710-003980   HF9603            SIB-I8
SIB 1            REV 05   710-003980   HF9577            SIB-I8
SIB 2            REV 05   710-003980   HF9540            SIB-I8
SIB 3            REV 05   710-003980   HF9550            SIB-I8
SIB 4            REV 05   710-003980   HF9592            SIB-I8
```

What it Means The command output is for a T640 routing node. The command output displays the SIB slot number, revision level, part number, serial number, and description. By default, SIB0 is the redundant SIB.

Displaying SIB Redundancy Information

Action To display the redundant SIB state, use the following CLI command:

user@host> **show chassis sib**

Sample Output

```
t320@host> show chassis sibs
Slot  State              Uptime
 0    Spare
 1    Online            2 days, 7 hours, 10 minutes, 13 seconds
 2    Online            2 days, 7 hours, 10 minutes, 13 seconds

t640@host> show chassis sibs
Slot  State              Uptime
 0    Spare
 1    Online            4 hours, 5 minutes, 47 seconds
 2    Online            4 hours, 5 minutes, 42 seconds
 3    Online            4 hours, 5 minutes, 37 seconds
 4    Online            4 hours, 5 minutes, 33 seconds
```

What it Means The command output is for a T320 router and a T640 routing node. On the T320 router, SIB1 and SIB2 are active (Online), while SIB0 is backup (Spare). On the T640 routing node, SIB1, SIB2, SIB3, and SIB4 are active, while SIB0 is the backup. The possible states are Spare, Online, Offline, or Empty. The command output also displays how long each SIB has been online in hours, minutes, and seconds.

Alternative Action You can also view redundant SIB status by using the following CLI command:

user@host> **show chassis environment sib**

```
user@host> show chassis environment sib
```

```
SIB 0 status:
  State                          Spare
  Temperature                 44 degrees C / 111 degrees F
  Power:
    GROUND                     0 mV
    1.8 V                   1807 mV
    2.5 V                   2478 mV
    3.3 V                   3308 mV
    1.8 V bias              1797 mV
    3.3 V bias              3284 mV
    5.0 V bias              5018 mV
    8.0 V bias              7440 mV
SIB 1 status:
  State                          Online
  Temperature                 50 degrees C / 122 degrees F
  Power:
    GROUND                     0 mV
    1.8 V                   1814 mV
    2.5 V                   2485 mV
1.8 V bias              1794 mV
    3.3 V bias              3313 mV
    5.0 V bias              5028 mV
    8.0 V bias              7553 mV
SIB 2 status:
  [...Output truncated...]
SIB 3 status:
  [...Output truncated...]
SIB 4 status:
  [...Output truncated...]
```

The command output displays the SIB slot, status, and the temperature of the air flowing past the SPP card and the power source information. Notice that SIB0 status is displayed as Spare, or backup.

You can display the environmental status of a particular SIB with the following CLI command:

user@host> **show chassis environment sib** *slot*

Monitoring Redundant SIB Status

Action To monitor the SIB status, see “Monitoring the SIB Status” on page 329.

Displaying SIB Alarms

Action To display SIB alarms, see “Displaying SIB Alarms” on page 332.

Performing a Swap Test on a SIB

SIBs are hot-insertable and hot-removable.

Action To perform a swap test on a SIB, see “Verifying SIB Failure” on page 334.

Returning the SIB

Action To return a SIB, locate the serial number label on the left side of the SIB top panel, then follow the procedure “Return the Failed Component” on page 86. You can also refer to the procedure to return a field-replaceable unit in the M320 router, T320 router, or the T640 routing node hardware guide.

Chapter 41

Monitoring Redundant SCGs

You monitor and maintain redundant SONET Clock Generators (SCGs) installed in the T320 router and the T640 routing node to ensure that there is no interruption of function. SCGs provide a clock signal for SONET/SDH, and select a clock signal from any Flexible PIC Concentrator (FPC), or from the external clock inputs.

Table 117 lists the tasks you perform to monitor redundant SCGs.

Table 117: Checklist for Monitoring the Redundant SCG

Monitor SCG Tasks	Command or Action
Understanding Redundant SCGs on page 552	
Displaying Redundant SCG Hardware Information on page 553	show chassis hardware
Monitoring Redundant SCG Status on page 553	
1. Monitor the Redundant SCG Environmental Status on page 553	show chassis environment show chassis environment scg
2. Display the Redundant SCG LED States at the Command Line on page 555	show chassis craft-interface
3. View the Redundant SCG LEDs on page 555	Remove the rear component cover and look on the SCG faceplate at the back of the T320 router or T640 routing node chassis.
Displaying Redundant SCG Mastership on page 555	
1. Display the SCG Master and Standby from the Craft Interface Output on page 556	show chassis craft-interface
2. View the SCG LEDs on page 556	Remove the rear component cover and look on the SCG faceplate at the rear of the T320 router or T640 routing node chassis.
Performing a Swap Test on a Redundant SCG on page 556	1. Take the SCG offline. request chassis scg offline slot number 2. Replace the SCG with one that you know works. 3. Bring the SCG online. request chassis scg offline slot number 4. Verify the SCG status. request chassis scg offline slot number
Returning the SCG on page 557	See “Return the Failed Component” on page 86, or follow the procedure in the M40e or M160 router hardware guide.

Understanding Redundant SCGs

Purpose Inspect redundant SCGs to ensure that they provide a clock signal for the SONET/SDH interfaces on the router and that they select a clock signal from any FPC, or from the external clock inputs.

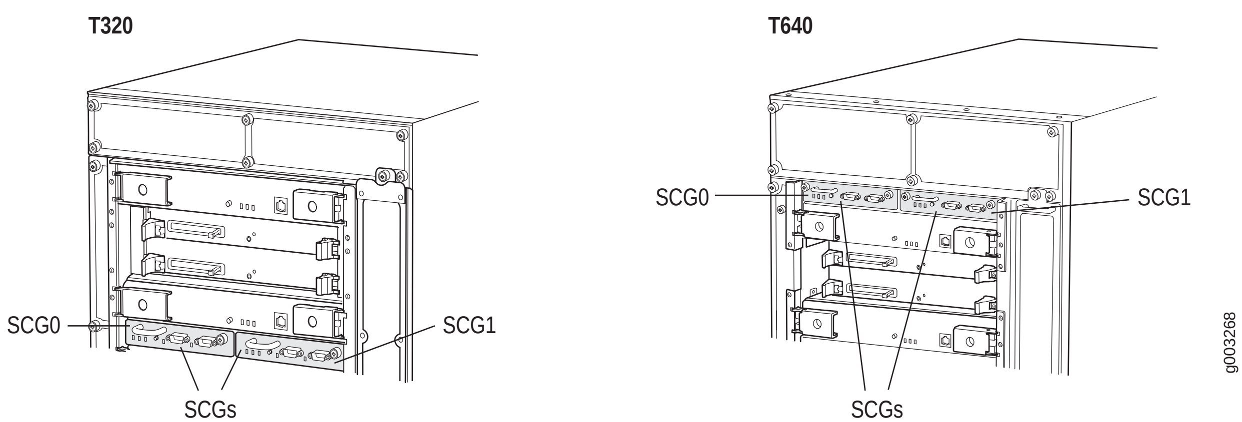
What Are Redundant SCGs Two SCGs are installed in the T320 router and the T640 routing node. The SCGs install into the upper rear of the chassis in the slots labeled SCG0 and SCG1.

If both SCGs are installed and functioning normally, SCG0 is master and SCG1 is backup. Removing the backup SCG does not affect the functioning of the routing node. Taking the master SCG offline can result in a brief loss of SONET clock lock while the backup SCG becomes master.

The SCGs are hot-pluggable.

Figure 226 shows the location of the SCGs on the T320 router and the T640 routing node.

Figure 226: T320 Router and T640 Routing Node Redundant SCG Location



See Also

- Monitoring the Host Subsystem on page 289
- Monitoring Redundant SCGs on page 551

Displaying Redundant SCG Hardware Information

Action To display the redundant SCG hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                abcdef            T320
Midplane         REV 01   710-004339   AY4529
FPM GBUS         REV 02   710-004461   AY4511
FPM Display      REV 02   710-002897   HF6094
CIP              REV 05   710-002895   HC0468
PEM 1            Rev 01   740-004359   2708013           Power Entry Module
SCG 0            REV 06   710-004455   AY4526
SCG 1            REV 06   710-004455   AY4523
```

What It Means The command output displays the SCG slot number, revision level, part number, and serial number.

Monitoring Redundant SCG Status

Steps To Take To monitor the redundant SCG status, follow these steps:

1. Monitor the Redundant SCG Environmental Status on page 553
2. Display the Redundant SCG LED States at the Command Line on page 555
3. View the Redundant SCG LEDs on page 555

Step 1: Monitor the Redundant SCG Environmental Status

Action To check the redundant SCG environment status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
t320@host> show chassis environment
Class Item                   Status     Measurement
Power PEM 0                  Absent
      PEM 1                  OK
Temp  SCG 0                  OK         30 degrees C / 86 degrees F
      SCG 1                  OK         29 degrees C / 84 degrees F
[...Output truncated...]
```

What It Means The command output displays the status and temperature for each SCG.

Alternative Action If there is a problem with the SCG status, you can display more detailed SCG environmental information with the following CLI command:

user@host> **show chassis environment scg**

The command output is as follows:

```
t320@host> show chassis environment scg
SCG 0 status:
  State                            Online -  Master clock
  Temperature                   30 degrees C / 86 degrees F
  Power:
    GROUND                       0 mV
    3.3 V                     3317 mV
    5.0 V                     5072 mV
    5.6 V                     5697 mV
    1.8 V bias                1794 mV
    3.3 V bias                3304 mV
    5.0 V bias                4991 mV
    8.0 V bias                7318 mV
  BUS Revision                  40
SCG 1 status:
  State                            Online - Standby
  Temperature                   29 degrees C / 84 degrees F
  Power:
    GROUND                       0 mV
    3.3 V                     3318 mV
    5.0 V                     5084 mV
    5.6 V                     5704 mV
    1.8 V bias                1782 mV
    3.3 V bias                3286 mV
    5.0 V bias                5003 mV
    8.0 V bias                7323 mV
  BUS Revision                  40
```

The command output displays the status for each SCG slot 0 and 1. The operating status can be Present, Online, Offline, or Empty. If Online, it can be the clock source (Master clock) or backup (Standby). As shown in the output, the redundant SCG is SCG1, with a status of Standby. The command output displays the temperature of the air flowing past the SCG. The command output also displays information about the SCG power supplies and the SCG circuitry revision level.

Step 2: Display the Redundant SCG LED States at the Command Line

Action To display the redundant SCG LED states, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
t320@host> show chassis craft-interface
[...Output truncated...]
SCG LEDs:
  SCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .
[...Output truncated...]
```

What It Means The command output displays the SCG LED status. The router has two SCGs installed. Asterisks (*) indicate the operation status. The color represents the possible SCG operating states: Amber (Fail), Green (OK), and Blue (Master). Both SCGs are functioning properly (Green). The SCG in slot 0 is operating as master; the SCG in slot 1 is the backup.

Step 3: View the Redundant SCG LEDs

Action To view the redundant SCG LEDs, remove the rear component cover and look on the SCG faceplate at the rear of the router chassis. Table 118 describes the functions of these LEDs.

Table 118: SCG LEDs

Label	Color	State	Description
OK	Green	On steadily	SCG is online and is functioning normally.
FAIL	Amber	On steadily	SCG has failed.
MASTER	Blue	On steadily	SCG is functioning as master.

Displaying Redundant SCG Mastership

If both SCGs are installed and functioning normally, SCG0 is master and SCG1 is backup. Removing the backup SCG does not affect the functioning of the routing node. Taking the master SCG offline might result in a brief loss of SONET clock lock while the backup SCG becomes master.

Steps To Take To determine which SCG is operating as the master and which is operating as the standby, follow these steps:

1. Display the SCG Master and Standby from the Craft Interface Output on page 556
2. View the SCG LEDs on page 556

Step 1: Display the SCG Master and Standby from the Craft Interface Output

Action To determine the SCG master and SCG standby from the craft interface status information, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
SCG LEDs:
  SCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .
[...Output truncated...]
```

What It Means The command output displays which SCG is operating as master. Asterisks (*) indicate the operation status. The color represents the possible SCG operating states: Amber (Fail), Green (OK), and Blue (Master). The SCG in slot 0 is operating as master; the SCG in slot 1 is the backup.

Step 2: View the SCG LEDs

Action Check the blue MASTER LED on the SCG faceplate. If this LED is on steadily, the SCG is functioning as master. Table 118 on page 555 describes the functions of the SCG LEDs.

Performing a Swap Test on a Redundant SCG

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SCG for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on a redundant SCG, follow these steps:

1. Take the SCG offline by doing one of the following:
   - Use the following CLI command:

     user@host> **request chassis scg offline slot** *number*

   - Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the ESD points on the chassis. Press the online/offline button on the SCG faceplate and hold it down until the LED goes out (about 5 seconds).
2. Loosen the captive screws on the edges of the SCG faceplate.
3. Grasp the SCG by the handle on the faceplate and slide it out of the chassis.
4. Place the SCG on the antistatic mat.

5. Remove the replacement SCG from its electrostatic bag.
6. Carefully align the sides of the SCG with the guides in the SCG slot.
7. Grasp the SCG by its handle and slide it straight into the chassis until it contacts the midplane.
8. Tighten the captive screws on the corners of the SCG faceplate.
9. Bring the SCG online by doing one of the following:
   - Use the following CLI command:

     user@host> r**equest chassis scg online slot** *number*

   - Press the online/offline button until the green ONLINE LED lights.
10. Verify that the SCG is online by using the following CLI command:

    user@host> **request chassis scg online slot** *number*

    If the replaced SCG is online, the removed SCG has failed. Return the SCG as described in “Return the Failed Component” on page 86.

Returning the SCG

Action To return an SCG, locate the serial number on the top of the SCG, close to the midplane connector. See “Return the Failed Component” on page 86, or the procedure to return a field-replaceable unit in the T320 router or T640 routing node hardware guide.

Chapter 42

Monitoring Redundant Control Boards

You monitor and maintain redundant Control Boards installed in the M320 router, T320 router, or T640 routing node to ensure that there is no interruption of functions such as the following:

- Router component monitoring and control for failure and alarm conditions
- Component power-up and power-down control
- Redundant Routing Engine and Control Board mastership control
- Flexible PIC Concentrator (FPC) error detection and reset control
- SONET clock source generation and monitoring
- SONET reference clock monitoring (from the FPC and BIT interfaces)
- I^2C controller monitoring
- Fan speed monitoring and control

For more information about monitoring a single Control Board, see "Monitoring the Control Board" on page 301.

Table 119 provides a checklist of tasks you perform to monitor redundant Control Boards.

Table 119: Checklist for Monitoring Redundant Control Boards

Monitor Redundant Control Board Tasks	Command or Action
Understanding Redundant Control Boards on page 561	
Displaying Redundant Control Board Hardware Information on page 563	show chassis hardware
Displaying Redundant Control Board Mastership on page 563	
1. Check the Redundant Control Board Environmental Status on page 564	show chassis environment cb
2. Check the Redundant Control Board Status from the Craft Interface on page 565	show chassis craft-interface
3. Check the Redundant Control Board LED Status on page 565	Examine the LEDs on the Control Board faceplate.

Monitor Redundant Control Board Tasks	Command or Action
Switching Control Board Mastership on page 565	Press the Control Board offline button on the component faceplate.
Checking the Control Board Alarms on page 565	See "Checking the Control Board Alarms" on page 308. For conditions that trigger Control Board alarms, see "Display the Current Router Alarms" on page 61.
Replacing a Control Board on page 566	1. Determine whether the host subsystem is functioning as master or as backup by using the show chassis routing-engine command. 2. Take the host subsystem offline if the Control Board is master by using the request chassis routing-engine master switch command. 3. Replace the Control Board with a known working one. 4. Check the Control Board status by examining the LEDs on the Control Board faceplate, or by using the show chassis hardware command.
Returning the Control Board on page 566	Locate the Control Board serial number ID label. See "Return the Failed Component" on page 86 or the appropriate hardware guide.

Understanding Redundant Control Boards

Purpose

Inspect redundant Control Boards to ensure that router component functions are uninterrupted. Each Control Board works with an adjacent Routing Engine to provide control and monitoring functions for the router. These include determining Routing Engine mastership; controlling power, reset, and SONET clocking for the other router components; monitoring and controlling fan speed; and monitoring system status.

What Are Redundant Control Boards

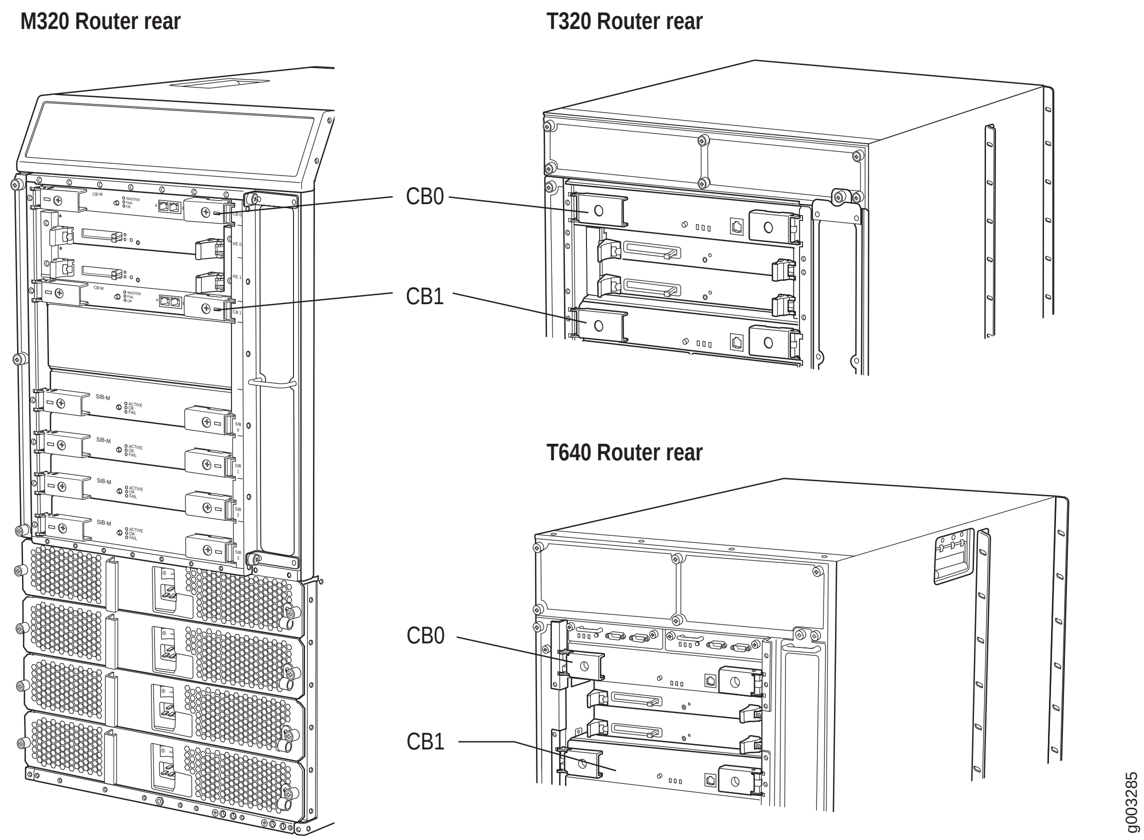
Redundant Control Boards are two Control Boards installed in the M320 router, T320 router, or the T640 routing node.

The Control Board is a component of the host module. Each Control Board requires a Routing Engine to be installed in an adjacent slot. The Control Board in slot CB0 installs above the Routing Engine in slot RE0, and the Control Board in slot CB1 installs below the Routing Engine in slot RE1. Even if a Control Board is physically installed in the chassis, it does not function if there is no Routing Engine present in the adjacent slot.

If two Control Boards are installed, by default, CB0 acts as the master Control Board and CB1 acts as a backup. If the master Control Board (CB0) fails or is removed, the backup (CB1) restarts and becomes the master Control Board.

The Control Boards install into the midplane from the back of the chassis (see Figure 227 on page 562). The Control Boards are hot-pluggable.

Figure 227: M320 Router, T320 Router, and T640 Routing Node Control Board Location



See Also

- Monitoring the Host Subsystem on page 289
- Monitoring the Routing Engine on page 125
- Monitoring the Control Board on page 301

Displaying Redundant Control Board Hardware Information

To display whether redundant Control Boards are installed in a router and to obtain hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
t640@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                abcdef            T320
Midplane         REV 01   710-004339   AY4529
FPM GBUS         REV 02   710-004461   AY4511
FPM Display      REV 02   710-002897   HF6094
CIP              REV 05   710-002895   HC0468
PEM 1            Rev 01   740-004359   2708013           Power Entry Module
SCG 0            REV 06   710-004455   AY4526
SCG 1            REV 06   710-004455   AY4523
Routing Engine 0 REV 01   740-005022   210929000142      RE-3.0
Routing Engine 1 REV 01   740-005022   210929000143      RE-3.0
CB 0             REV 06   710-002728   HC0065
CB 1             REV 05   710-002728   HE3623
[...Output truncated...]
```

What It Means The command output displays the Control Boards installed in the router chassis, including the slot number, revision level, part number, serial number, and a brief description of the component. Give this information to the Juniper Networks Technical Assistance Center (JTAC) if a Control Board fails. The command output for this T640 routing node shows that two Control Boards are installed. By default, CB1 is the redundant Control Board.

Displaying Redundant Control Board Mastership

Steps To Take To display Control Board mastership, do one of the following:

1. Check the Redundant Control Board Environmental Status on page 564
2. Check the Redundant Control Board Status from the Craft Interface on page 565
3. Check the Redundant Control Board LED Status on page 565

Step 1: Check the Redundant Control Board Environmental Status

Action To check the redundant Control Board environmental status, use the following CLI command:

user@host> **show chassis environment cb**

Sample Output

```
t640@host> show chassis environment cb
CB 0 status:
  State                           Online Master
  Temperature                  29 degrees C / 84 degrees F
  Power:
    1.8 V                    1805 mV
    2.5 V                    2501 mV
    3.3 V                    3293 mV
    4.6 V                    4725 mV
    5.0 V                    5032 mV
    12.0 V                  11975 mV
    3.3 V bias               3286 mV
    8.0 V bias               7589 mV
  GBUS Revision                40
  FPGA Revision                 7
CB 1 status:
  State                           Online Standby
  Temperature                  32 degrees C / 89 degrees F
  Power:
    1.8 V                    1802 mV
    2.5 V                    2482 mV
    3.3 V                    3289 mV
    4.6 V                    4720 mV
    5.0 V                    5001 mV
    12.0 V                  11946 mV
    3.3 V bias               3274 mV
    8.0 V bias               7562 mV
  GBUS Revision                40
  FPGA Revision                 7
```

What It Means The command output displays which Control Board is master and standby. Additionally, the command output displays the Control Board state, redundancy status, temperature, power source, and circuitry revision level for each Control Board installed in the router chassis. CB1 is shown in standby mode, and is the redundant Control Board.

Alternative Action To display the environmental status of a particular Control Board, use the following JUNOS CLI operational mode command:

t640@host> **show chassis environment cb** *slot*

Step 2: Check the Redundant Control Board Status from the Craft Interface

Action If you are near the router, physically look at the craft interface for the Control Board LEDs. To display redundant Control Board status from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
t640@host> show chassis craft-interface
FPM Display contents:
[...Output truncated...}
CB LEDs:
   CB   0   1
--------------
Amber  .
Green  *
Blue   *
[...Output truncated...]
```

What It Means The CB LEDs section of the command output indicates the status of the redundant Control Board. An asterisk (*) indicates the current operating state: Amber (offline), Green (online), and Blue (Master). In the above output, no redundant Control Board is installed—the output under CB1 is blank.

Step 3: Check the Redundant Control Board LED Status

Action To check the redundant Control Board LED status, look at the three LEDs located on the Control Board faceplate. Table 120 describes the Control Board LED states.

Table 120: Control Board LEDs

Label	Color	State	Description
OK	Green	On steadily	Control Board is online and is functioning normally.
FAIL	Amber	On steadily	Control Board has failed.
MASTER	Blue	On steadily	Control Board is functioning as master.

Switching Control Board Mastership

Action To switch the Control Board master to backup or the Control Board backup to master, take the Control Board offline by pressing the Control Board offline button on the component faceplate. The backup Control Board will automatically start up. To remove the Control Board, see "Replacing a Control Board" on page 566.

Checking the Control Board Alarms

Action To check for the Control Board alarms, see "Checking the Control Board Alarms" on page 308. For conditions that trigger Control Board alarms, see "Display the Current Router Alarms" on page 61.

Replacing a Control Board

The Control Board can fail and not start, or it can cause a connectivity problem between the Routing Engine and the Packet Forwarding Engine components. You can perform a swap test on the Control Board to try to pinpoint the problem.

Action To replace a Control Board, see "Component Fuses in the M320 Router Midplane" on page 311.

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the Control Board for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Returning the Control Board

Action To return the Control Board, follow these steps:

1. Locate the serial number ID label on the bottom of the left side of the Control Board (see "Locate the Control Board Serial Number ID Label" on page 314).

2. Follow the procedure "Return the Failed Component" on page 86. You can also refer to the procedure to return a field-replaceable unit in the M320 router, T320 router, or the T640 routing node hardware guides.

Chapter 43

Monitoring Redundant MCSs

You monitor and maintain redundant Miscellaneous Control Subsystems (MCSs) installed in the M40e or M160 router to ensure that there is no interruption of functions such as the following:

- Router component monitoring and control for failure and alarm conditions
- Component power-up and power-down control
- Redundant Routing Engine, MCS, and PFE Clock Generator (PCG) mastership control
- Flexible PIC Concentrator (FPC) error detection and reset control
- SONET clock source generation and monitoring
- SONET reference clock (from the FPC and BIT interfaces) monitoring
- System clocks (from the PCG) monitoring

For more information about monitoring a single MCS, see "Monitoring the MCS" on page 359.

Table 121 provides a checklist of tasks you perform to monitor redundant MCSs.

Table 121: Checklist for Monitoring Redundant MCSs

Monitor Redundant MCS Tasks	Command or Action
Understanding Redundant MCSs on page 569	
Displaying Redundant MCS Hardware Information on page 570	show chassis hardware
Monitoring Redundant MCS Status on page 570	
1. Check the Redundant MCS Environmental Status on page 571	show chassis environment mcs
2. Check the Redundant MCS Status from the Craft Interface on page 572	show chassis craft-interface
3. Check the Redundant MCS LED Status on page 573	Check the LEDs on the MCS faceplate.

Monitor Redundant MCS Tasks	Command or Action
Displaying Redundant MCS Mastership on page 573	
1. Check the Redundant MCS Environmental Status on page 571	show chassis environment mcs
2. Check the Redundant MCS Status from the Craft Interface on page 572	show chassis craft-interface
3. Check the Redundant MCS LED Status on page 573	Check the LEDs on the MCS faceplate.
Switching MCS Mastership on page 573	Manually take the MCS offline by pressing the offline button on the component faceplate.
Performing a Swap Test on a Redundant MCS on page 573	1. Take the host module offline. 2. Take the MCS offline. 3. Remove the MCS and replace it with one that you know works.
Returning an MCS on page 575	See "Return the Failed Component" on page 86, or follow the procedure in the M40e or M160 router hardware guide.

Understanding Redundant MCSs

Purpose Inspect redundant MCSs to ensure that functions are interrupted, such as component alarm messages; component power-up and power-down; Routing Engine, MCS, and PCG mastership control; SONET clock generation and monitoring; and system clock monitoring.

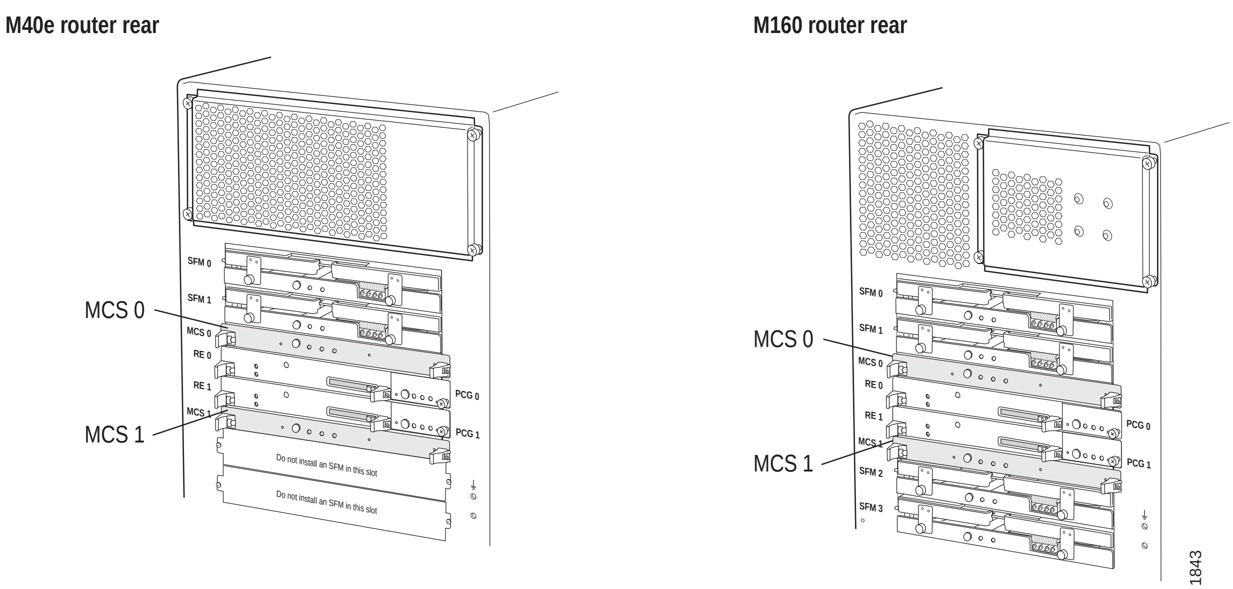
What Are Redundant MCSs Redundant MCSs are two MCSs installed in the M40e or M160 router.

The MCS is a component of the host module. Each MCS requires a Routing Engine to be installed in an adjacent slot. MCS0 installs above slot RE0, and MCS1 installs below slot RE1. Even if an MCS is physically installed in the chassis, it does not function if there is no Routing Engine present in the adjacent slot.

If two MCSs are installed, MCS0 acts as the master MCS and MCS1 acts as a backup. If the master MCS fails or is removed, the backup restarts and becomes the master MCS.

The MCSs install into the midplane from the back of the chassis (see Figure 228).

Figure 228: M40e and M160 Router Redundant MCSs



See Also

- Monitoring the Host Module on page 341
- Monitoring the MCS on page 359
- Monitoring Redundant Routing Engines on page 491

Displaying Redundant MCS Hardware Information

Action To display whether there are redundant MCSs installed in a router and to get hardware information, use the following command-line interface (CLI) command:

user@ host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                51029             M160
Midplane         REV 05   710-001245   AW3223
FPM CMB          REV 03   710-001642   AH5190
FPM Display      REV 03   710-001647   AW2021
CIP              REV 04   710-002649   AG5779
PEM 0            Rev 03   740-001243   LK16612           Power Entry Module
PEM 1            Rev 03   740-001243   LK16604           Power Entry Module
PCG 0            REV 07   710-001568   HF1164
PCG 1            REV 07   710-001568   HF1159
Routing Engine 0 REV 01   740-003239   AARCHOO           RE-2.0
Routing Engine 1 REV 01   740-003239   AARCHOO           RE-2.0
MCS 0            REV 11   710-001226   AV4425
MCS 1            REV 11   710-001226   HD2842
[...Output truncated...]
```

What It Means The command output displays the MCS slot number, revision level, part number, and serial number. Give this information to the Juniper Networks Technical Assistance Center (JTAC) if an MCS fails.

Monitoring Redundant MCS Status

Steps To Take To monitor redundant MCSs, do one of the following:

1. Check the Redundant MCS Environmental Status on page 571
2. Check the Redundant MCS Status from the Craft Interface on page 572
3. Check the Redundant MCS LED Status on page 573

Step 1: Check the Redundant MCS Environmental Status

Action To check the redundant MCS status, use the following CLI command:

user@host> **show chassis environment mcs**

Sample Output

```
user@host> show chassis environment mcs
MCS 0 status:
  State                          Online Master
  Temperature                  0 degrees C / 32 degrees F
  Power:
    3.3 V                   3318 mV
    5.0 V                   5001 mV
    12.0 V                 11833 mV
    5.0 V bias              4991 mV
    8.0 V bias              8341 mV
  CMB Revision                12
  FPGA Revision               12
MCS 1 status:
  State                          Present
  Power:
    3.3 V                   3308 mV
    5.0 V                   5013 mV
    12.0 V                 11809 mV
    5.0 V bias              4952 mV
    8.0 V bias              8346 mV
  CMB Revision                12
```

What It Means The show chassis environment mcs CLI command is available on the M40e and M160 routers only. The command output displays environmental information about both MCSs installed in the router or about an individual MCS. The MCS status can be Present, Online, Offline, or Empty. The command also indicates that the MCS is the master MCS. The command output also displays the temperature of the air flowing past the MCS, information about MCS power supplies, field-programmable gate array (FPGA) revision information, and the revision level of the chassis management bus (CMB) slave.

Alternative Action To display the environmental status of a particular MCS, use the following JUNOS CLI operational mode command:

user@host> **show chassis environment mcs** *slot*

Step 2: Check the Redundant MCS Status from the Craft Interface

Action To display redundant MCS status from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
FPM Display contents:
    +--------------------+
    |myrouter            |
    |3 Alarms active     |
    |R: Hard errors      |
    |R: PEM 1 Input Fail |
    +--------------------|

Front Panel System LEDs:
Routing Engine    0    1
--------------------------
OK                *    *
Fail              .    .
Master            *    .

Front Panel Alarm Indicators:
-----------------------------
Red LED      *
Yellow LED   *
Major relay  *
Minor relay  *

Front Panel FPC LEDs:
FPC    0   1   2   3   4   5   6   7
------------------------------------
Red    *   .   .   .   *   .   .   .
Green  .   *   .   *   .   *   *   .

MCS LEDs:
  MCS   0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

[...Output truncated...]
```

What It Means The MCS LEDs section of the command output indicates the status of the redundant MCSs. An asterisk (*) indicates the current operating state: Amber (offline), Green (online), and Blue (Master).

Step 3: Check the Redundant MCS LED Status

Action To check redundant MCS LED status, look on the faceplate of the MCS at the rear of the router. Table 122 describes the LED states.

Table 122: MCS LEDs

Color	Label	State	Description
Blue	MASTER	On steadily	MCS is master.
Green	OK	On steadily	MCS is operating normally.
		Blinking	MCS is starting up.
Amber	FAIL	On steadily	MCS has failed.

When the MCS is functioning normally, the green OK LED remains on steadily.

Displaying Redundant MCS Mastership

Steps To Take To display which MCS is master and which is backup, do one of the following:

1. Check the Redundant MCS Environmental Status on page 571
2. Check the Redundant MCS Status from the Craft Interface on page 572
3. Check the Redundant MCS LED Status on page 573

Each step displays the master and backup MCS.

Switching MCS Mastership

Action To switch the MCS master to backup or the MCS backup to master, take the MCS offline by pressing the MCS offline button on the component faceplate. The backup MCS will automatically start up. To remove the MCS, see “Performing a Swap Test on a Redundant MCS” on page 573.

Performing a Swap Test on a Redundant MCS

The MCS can fail and not start, or it can cause a connectivity problem between the Routing Engine and the Packet Forwarding Engine components, such as the FPC and Switching and Forwarding Module (SFM). You can perform a swap test on the MCS to try to pinpoint the problem.

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the MCS for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on the MCS, remove it and replace it with one that you know works.

Normally, if two host modules are installed in the router, HOST0 functions as the master and HOST1 as the backup. You can remove the backup host module (or either of its components) without interrupting the functioning of the router. If you take the master host module offline, the router reboots and the backup host module becomes the master. If the router has only one host module, taking it offline causes the router to shut down.

The host module is taken offline and brought back online as a unit. Before you replace the Routing Engine or an MCS, you must take the host module offline. The host module is hot-pluggable.

To remove an MCS, follow these steps:

1. Lay an electrostatic bag or antistatic mat on a flat, stable surface to receive the Routing Engine.

2. Attach an electrostatic discharge (ESD) strap to your bare wrist and connect the strap to one of the ESD points on the chassis.

3. Remove the rear component cover by loosening the screws at the corners of the cover and pulling it straight off of the chassis.

4. If two host modules are installed, check whether the MCS you are removing belongs to the master host module with the following CLI command:

   user@host> **show chassis environment mcs**

   Or you can check the MCS LEDs. If the MCS belongs to the master host module, switch mastership to the standby host module by including the routing-engine statement at the [edit chassis redundancy] hierarchy level in the configuration, as described in the *JUNOS System Basics Configuration Guide*.

5. On the console or other management device connected to the Routing Engine that is paired with the MCS you are removing, enter CLI operational mode and issue the following command:

   user@host> **request system halt**

   The command shuts down the Routing Engine cleanly, so its state information is preserved.

   Wait to continue until all software processes have shut down.

6. Flip the ends of the extractor clips outward.

7. Grasp the extractor clips and slide the unit about halfway out of the chassis.

8. Place one hand under the MCS to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.

9. Align the rear of the MCS with the guides inside the chassis and slide it in completely.

10. Press the extractor clips on the left and right sides of the MCS inward.

11. Verify that the green LED labeled OK on the MCS faceplate is lit. Also check the host module LEDs on the craft interface to verify that the green LED labeled ONLINE is lit for the host module to which the MCS belongs.

12. Verify correct MCS functioning by using the show chassis environment mcs command.

If the replacement MCS works, you can be certain that the replaced MCS failed. To return the MCS, see “Returning an MCS” on page 575.

Returning an MCS

Action To return an MCS, see “Return the Failed Component” on page 86, or the procedure to return a field-replaceable unit in the M40e or M160 router hardware guide.

Chapter 44

Monitoring Redundant SFMs

You monitor redundant Switching and Forwarding Modules (SFMs) to ensure that traffic transiting the router is handled properly. SFMs contain the Internet Processor II application-specific integration circuits (ASICs), which make forwarding decisions, and the Distributed Buffer Manager ASICs, which distribute data cells throughout memory and forward notification of outgoing packets. (See Table 123.)

Table 123: Checklist for Monitoring Redundant SFMs

Monitor Redundant SFM Tasks	Command or Action
Understanding Redundant SFMs on page 579	
Understanding M40e Router Redundant SFM Configuration on page 580	
Understanding M40e Router Redundant SFM Operation on page 580	
Understanding M160 Router Redundant SFM Operation on page 580	
Displaying Redundant SFM Hardware Information on page 581	show chassis hardware
Monitoring Redundant SFM Status on page 581	
1. Display the SFM Summary Status on page 582	show chassis sfm *sfm-slot* show chassis sfm detail *sfm-slot*
2. Display the SFM LED Status at the Command Line on page 584	show chassis craft-interface
3. Check the SFM LED Status on the Faceplate on page 584	Check the SFM faceplate at the back of the M40e and M160 router chassis.
4. Display the SFM Environmental Status on page 585	show chassis environment show chassis environment sfm *slot*
Displaying Redundant SFM Mastership on page 587	
1. Display SFM Mastership at the Command Line on page 587	show chassis sfm
2. Display SFM Mastership Information from the Craft Interface on page 588	show chassis craft-interface
Displaying Redundant SFM Alarms on page 588	
1. Display the Current Redundant SFM Alarms on page 588	show chassis alarms
2. Display SFM Error Messages in the System Log File on page 589	show log messages
3. Display SFM Error Messages in the Chassis Daemon Log File on page 589	show log chassisd | match sfm

Monitor Redundant SFM Tasks	Command or Action
Verifying SFM Failure on page 590	
1. Check the SFM Connection on page 590	Check the thumbscrews on the SFM ejector locking tabs.
2. Restart the SFM on page 590	request chassis sfm slot *slot-number* restart
3. Perform an SFM Swap Test on page 591	1. Take the SFM offline. 2. Replace the SFM with one that you know works. 3. Bring the SFM online. 4. Check the SFM status by using the show chassis sfm CLI command.
Controlling Redundant SFMs on page 591	
1. Take an SFM Offline on page 592	request chassis sfm slot *slot-number* offline
2. Bring an SFM Online on page 592	request chassis sfm slot *slot-number* online
3. Switch SFM Mastership on page 593	(M40e router only) request chassis sfm master switch <no-confirm>
Replacing an SFM on page 593	1. Take the SFM offline. 2. Remove the failed SFM. 3. Install a new SFM. 4. Bring the SFM online. 5. Verify that SFM is online by using the show chassis sfm CLI command.

Understanding Redundant SFMs

Purpose Inspect redundant SFMs to ensure that all traffic leaving the Flexible PIC Concentrators (FPCs) is handled properly.

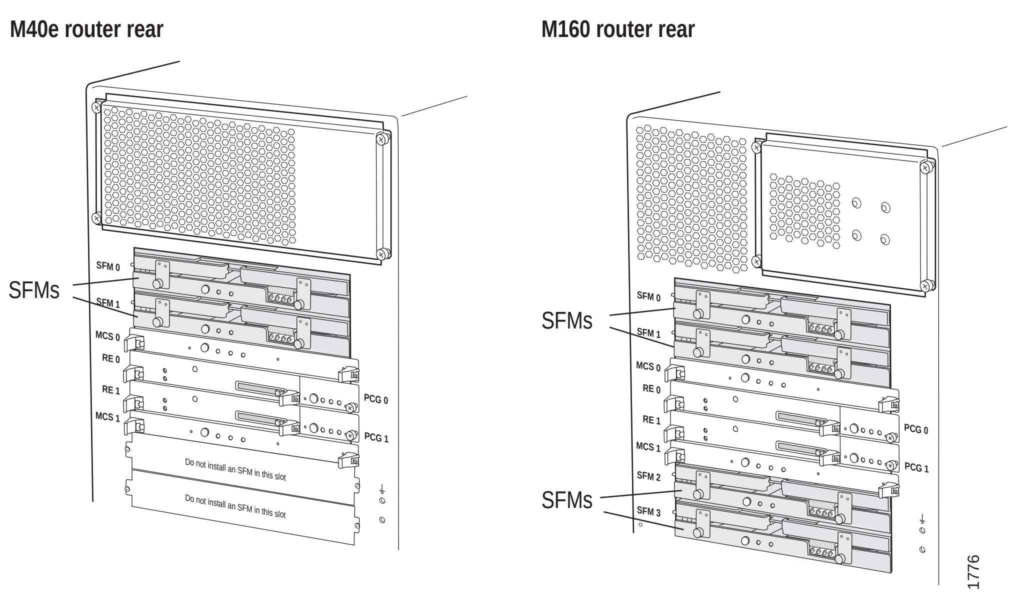
What Are Redundant SFMs SFMs are control boards that handle traffic transiting the router. The SFMs provide route lookup, filtering, and switching.

Up to four interconnected SFMs can be installed in the M160 router, providing a total of 160 million packets per second (Mpps) of forwarding. Up to two SFMs can be installed in the M40e router. Each SFM can process 40 Mpps.

The SFM is a two-board system containing the Switch Plane Processor (SPP) card and the Switch Plane Router (SPR) card. When the serial stream of bits leaves the FPC, it is directed to one of the SFMs. The Distributed Buffer Manager ASIC on the SFM distributes the data cells throughout memory banks that are shared over all FPCs. The Internet Processor II ASIC on the SFM performs route lookups and makes forwarding decisions. The Internet Processor II ASIC notifies a second Distributed Buffer Manager ASIC SFM, which forwards the notifications to the outbound interface. Each SFM effectively handles from one-half to one-quarter of the traffic on each FPC.

The SFMs are hot-removable and hot-insertable. Inserting or removing an SFM causes a brief interruption in forwarding performance (about 500 ms) as the Packet Forwarding Engine reconfigures the distribution of packets across the remaining SFMs.

Figure 229: M40e and M160 Router SFM Location



Understanding M40e Router Redundant SFM Configuration

You can configure which SFM is the master and which is the backup. By default, the SFM in slot 0 is the master and the SFM in slot 1 is the backup. You can modify the default configuration by including the sfm statement at the [edit chassis redundancy] hierarchy level.

NOTE: We recommend that both Routing Engines have the same configuration.

To display the current SFM redundancy configuration, follow these steps:

1. Enter the CLI configuration mode using the following command:

   user@host# **configure**

2. Go to the [edit chassis redundancy] hierarchy level.

3. Show the SFM configuration using the following command:

   user@host# **show**

Understanding M40e Router Redundant SFM Operation

One or two SFMs can be installed into the midplane from the rear of the M40e router chassis, as shown in Figure 229 on page 579. Only one SFM is active at a time, with the optional second SFM in standby mode. Removing the standby SFM has no effect on router function. If the active SFM fails or is removed from the chassis, what happens depends on the number of SFMs installed:

- If there is only one SFM, forwarding halts until the SFM is replaced and online.
- If there are two SFMs, forwarding halts until the standby SFM boots and becomes active.

It takes approximately 1 minute for the new SFM to become active. Synchronizing router configuration information can take additional time, depending on the complexity of the configuration.

Understanding M160 Router Redundant SFM Operation

Up to four SFMs can be installed into the midplane from the rear of the M160 router chassis, as shown in Figure 229 on page 579. All SFMs are active at the same time. A failure or taking an SFM offline has no effect on router function unless it is the only SFM installed. If only one SFM is installed, forwarding halts until the SFM is replaced and is back online. If two or more SFMs are installed, forwarding continues uninterrupted.

Displaying Redundant SFM Hardware Information

Action To display redundant SFM hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output For M40e routers:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                                  M40e
[...Output truncated...]
SFM 0 SPP        REV 07   710-001228   AF2247
SFM 0 SPR        REV 05   710-002189   AF1847            Internet Processor II
SFM 1 SPP        REV 07   710-001228   BE0175
SFM 1 SPR        REV 05   710-002189   BE0201            Internet Processor II
```

For M160 routers:

```
user@host> show chassis hardware
Item             Version  Part number  Serial number     Description
Chassis                                20079             M160
[...Output truncated...]
SFM 0 SPP        REV 04   710-001228   AA2860
SFM 0 SPR        REV 01   710-001224   AB0139            Internet Processor I
SFM 1 SPP        REV 04   710-001228   AA2859
SFM 1 SPR        REV 02   710-001224   AA9861            Internet Processor I
SFM 2 SPP        REV 06   710-001228   AB3082
SFM 2 SPR
SFM 3 SPP        REV 04   710-001228   AA1998
SFM 3 SPR        REV 01   710-001224   AB0137            Internet Processor I
[...Output truncated...]
```

What it Means The command output displays the SFM slot number and SFM serial component (SPP and SPR) card names, and the SFM revision level, part number, serial number, and description.

Monitoring Redundant SFM Status

Steps To Take To monitor the SFM status, follow these steps:

1. Display the SFM Summary Status on page 582
2. Display the SFM LED Status at the Command Line on page 584
3. Check the SFM LED Status on the Faceplate on page 584
4. Display the SFM Environmental Status on page 585

Step 1: Display the SFM Summary Status

Action To display the SFM summary status, use the following CLI command:

user@host> **show chassis sfm**

Sample Output For M40e routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           37      3          0        64        16         46
  1  Online - Standby  41      3          0        64        16         46
```

For M160 routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           41      2          0        64        16         46
  1  Offline            --- Hard FPC error ---
  2  Online           43      2          0        64        16         46
  3  Online           44      2          0       128         7         46
```

What it Means The command output displays the SFM slot number and the operating status of each SFM as Online, Offline, Present, or Empty.

The command output displays the temperature of air passing by the SFM, in degrees Centigrade. It displays the SFM CPU usage, including the total percentage used by the SFM processor and the percentage used for interrupts.

The command output also displays the percentage of memory usage, including the total DRAM available to the SFM processor, in megabytes (MB), and the percentage of heap space (dynamic memory) being used by the SFM processor. Heap utilization greater than 80 percent can indicate a software problem (memory leak). The output shows the percentage of buffer space being used by the SFM processor for buffering internal messages.

Alternative Action If the SFM summary command output indicates that there is a problem, you can display more detailed SFM status information with the following CLI command:

user@host> **show chassis sfm detail**

For M40e routers:

```
user@host> show chassis sfm detail
Slot 0 information:
  State                          Online
  SPP Temperature             37 degrees C / 98 degrees F
  SPR Temperature             41 degrees C / 105 degrees F
  Total CPU DRAM              64 MB
  Total SSRAM                  8 MB
  Internet Processor II          Version 1, Foundry IBM, Part number 9
  Start time:                    2002-09-03 19:55:51 PDT
  Uptime:                        3 hours, 47 minutes, 46 seconds
```

```
Slot 1 information:
  State                         Online - Standby
  SPP Temperature            41 degrees C / 105 degrees F
  SPR Temperature            40 degrees C / 104 degrees F
  Total CPU DRAM             64 MB
  Total SSRAM                 8 MB
  Internet Processor II         Version 1, Foundry IBM, Part number 9
```

For M160 routers:

```
Slot 0 information:
  State                         Online
  SPP Temperature            39 degrees C / 102 degrees F
  SPR Temperature            41 degrees C / 105 degrees F
  Total CPU DRAM             64 MB
  Total SSRAM                 4 MB
  Internet Processor I          Version 1, Foundry IBM, Part number 3
  Start time:                   2002-06-27 18:49:44 PDT
  Uptime:                       68 days, 4 hours, 55 minutes, 5 seconds
Slot 1 information:
  State                         Online
[...Output truncated...]
Slot 2 information:
  State                         Offline
[...Output truncated...]
Slot 3 information:
  State                         Online
[...Output truncated...]

Packet scheduling mode : Disabled
```

In addition to the command output displayed for the show chassis sfm command, the show chassis sfm detail command displays the temperature of air passing by the SPP and SPR cards (the two SFM serial components), in degrees Centigrade. It displays the total CPU DRAM and SRAM being used by the SFM processor. The command output displays the time that the SFM became active and how long the SFM has been up and running. A small uptime means that the SFM came online a short time ago and could indicate a possible SFM error condition.

To display the status of a particular SFM, use the following CLI command:

user@host> **show chassis sfm** *sfm-slot*

To display detailed status information about a particular SFM, use the following CLI command:

user@host> **show chassis sfm detail** *sfm-slot*

Step 2: Display the SFM LED Status at the Command Line

Action To display the SFM LED status, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output For M40e routers:

```
user@host> show chassis craft-interface
[...Output truncated...]
SFM LEDs:
  SFM  0   1
---------------
Amber  .   .
Green  *   *
Blue   *   .
```

For M160 routers:

```
user@host> show chassis craft-interface
[...Output truncated...]
SFM LEDs:
  SFM  0   1   2   3
-----------------------
Amber  .   .   *   .
Green  *   *   .   *
Blue   *   *   .   *
```

What it Means In the sample output for an M160 router, the SFMs in slots 0 and 1 are online and functioning normally. The status colors represent the possible SFM operating states: Amber (Fail), Green (OK), and Blue (Master). The (*) indicates the current operating state. There are no SFMs in slots 2 and 3.

Step 3: Check the SFM LED Status on the Faceplate

Action To check the SFM LED status, remove the component cover and look on the SFM faceplate at the back of the M40e or M160 router. Table 124 describes the SFM LED states.

Table 124: SFM LEDs

Color	Label	State	Description
Green	OK	On steadily	SFM is functioning normally.
		Blinking	SFM is starting up.
Amber	FAIL	On steadily	SFM has failed.

Step 4: Display the SFM Environmental Status

Action To display the SFM environmental information, use the following CLI command:

user@host> **show chassis environment**

Sample Output For M40e routers:

```
user@host> show chassis environment
Class Item                   Status     Measurement
Power PEM 0                  OK
      PEM 1                  Check
Temp  PCG 0                  OK         37 degrees C / 98 degrees F
      PCG 1                  OK         37 degrees C / 98 degrees F
      Routing Engine 0       OK         29 degrees C / 84 degrees F
      MCS 0                  OK         40 degrees C / 104 degrees F
      SFM 0 SPP              OK         37 degrees C / 98 degrees F
      SFM 0 SPR              OK         41 degrees C / 105 degrees F
      SFM 1 SPP              OK         41 degrees C / 105 degrees F
      SFM 1 SPR              OK         40 degrees C / 104 degrees F
[...Output truncated...]
```

For M160 routers:

```
user@host> show chassis environment
Class Item                   Status     Measurement
Power PEM 0                  OK
      PEM 1                  OK
Temp  [...Output truncated...]
      SPP 0                  OK         37 degrees C / 98 degrees F
      SPR 0                  OK         46 degrees C / 114 degrees F
      SPP 1                  OK         38 degrees C / 100 degrees F
      SPR 1                  OK         48 degrees C / 118 degrees F
      SPP 2                  OK         39 degrees C / 102 degrees F
      SPR 2                  OK         54 degrees C / 129 degrees F
      SFM 3                  Offline
      [...Output truncated...]
```

What it Means The command output displays the status and temperature for the SFM and its two serialized components: the SPP and SPR cards.

Alternative Actions If there is a problem with the SFM status, you can display more detailed environmental information with the following CLI command:

user@host> **show chassis environment sfm**

For M40e routers:

```
SFM 0 status:
  State                         Online
  SPP temperature            37 degrees C / 98 degrees F
  SPR temperature            41 degrees C / 105 degrees F
  SPP Power:
    1.5 V                  1501 mV
    2.5 V                  2495 mV
    3.3 V                  3293 mV
    5.0 V                  5042 mV
    5.0 V bias             4998 mV
```

```
  SPR Power:
    1.5 V                     1504 mV
    2.5 V                     2499 mV
    3.3 V                     3297 mV
    5.0 V                     5050 mV
    5.0 V bias                5008 mV
    8.0 V bias                8288 mV
  CMB Revision                  12
SFM 1 status:
  State                          Online - Standby
  SPP temperature               41 degrees C / 105 degrees F
  SPR temperature               40 degrees C / 104 degrees F
  SPP Power:
    1.5 V                     1498 mV
    2.5 V                     2468 mV
    3.3 V                     3296 mV
    5.0 V                     5042 mV
    5.0 V bias                4993 mV
  SPR Power:
    1.5 V                     1496 mV
    2.5 V                     2471 mV
    3.3 V                     3299 mV
    5.0 V                     5037 mV
    5.0 V bias                4996 mV
    8.0 V bias                8266 mV
  CMB Revision                  12
```

For M160 routers:

```
SFM 0 status:
  State                          Online
  SPP temperature               36 degrees C / 96 degrees F
  SPR temperature               45 degrees C / 113 degrees F
  SPP Power:
    1.5 V                     1501 mV
    2.5 V                     2485 mV
    3.3 V                     3291 mV
    5.0 V                     5020 mV
    5.0 V bias                4974 mV
  SPR Power:
    1.5 V                     1501 mV
    2.5 V                     2492 mV
    3.3 V                     3301 mV
    5.0 V                     5028 mV
    5.0 V bias                4986 mV
    8.0 V bias                8305 mV
  CMB Revision                  12
SFM 1 status:
  [...Output truncated...]
SFM 2 status:
  [...Output truncated...]
SFM 3 status:
  State                          Offline
 - Hard FPC error
  [...Output truncated...]
```

The command output displays the SFM slot, status, and the temperature of the air flowing past the SPP and SPR cards. It also displays information about the SFM power supplies. The chassis management bus (CMB) slave revision level is also displayed.

You can display the environmental status of a particular SFM with the following CLI command:

user@host> **show chassis environment sfm** *slot*

Displaying Redundant SFM Mastership

Steps To Take (For M40e routers only) To display which SFM is master, follow these steps:

1. Display SFM Mastership at the Command Line on page 587

2. Display SFM Mastership Information from the Craft Interface on page 588

Step 1: Display SFM Mastership at the Command Line

Action To display the SFM summary status at the command line, use the following CLI command:

user@host> **show chassis sfm**

Sample Output For M40e routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            37      3          0        64        16         46
  1  Online - Standby  41      3          0        64        16         46
```

For M160 routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            41      2          0        64        16         46
  1  Offline             --- Hard FPC error ---
  2  Online            43      2          0        64        16         46
  3  Online            44      2          0       128         7         46
```

What It Means The command output displays the SFM slot number and the operating status of each SFM as Online, Offline, Present, or Empty.

The command output displays the temperature of air passing by the SFM, in degrees Centigrade. It displays the SFM CPU usage, including the total percentage used by the SFM processor and the percentage used for interrupts.

The command output also displays the percentage of memory usage, including the total DRAM available to the SFM processor, in MB, and the percentage of heap space (dynamic memory) being used by the SFM processor. Heap utilization greater than 80 percent can indicate a software problem (memory leak). The output shows the percentage of buffer space being used by the SFM processor for buffering internal messages.

Step 2: Display SFM Mastership Information from the Craft Interface

Action To display SFM mastership information from the craft interface, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
SFM LEDs:
  SFM  0   1
---------------
Amber  .   .
Green  *   *
Blue   *   .
```

What It Means The command output shows that the SFM in slot 0 is online and functioning as the master. The status colors represent the possible SFM operating states: Amber (Fail), Green (OK), and Blue (Master). The (*) indicates the current operating state.

Displaying Redundant SFM Alarms

Steps To Take To display SFM alarms and error messages, follow these steps:

1. Display the Current Redundant SFM Alarms on page 588
2. Display SFM Error Messages in the System Log File on page 589
3. Display SFM Error Messages in the Chassis Daemon Log File on page 589

Step 1: Display the Current Redundant SFM Alarms

Action To display the current SFM alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
4 alarms currently active
Alarm time              Class  Description
2002-05-14 09:23:58 PDT  Major  SFM Failure
2002-05-14 09:23:55 PDT  Major  SFM Failure
2002-05-14 09:23:53 PDT  Major  SFM Failure
2002-05-14 09:20:51 PDT  Major  No SFM Online, the box is not forwarding
```

What It Means The command output displays the alarm date, time, severity level, and description.

Step 2: Display SFM Error Messages in the System Log File

Action To display the SFM error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jun 11 20:31:11 hissy-re0 craftd[556]:  Major alarm set, No SFM Online, the box
is not forwarding
Jun 11 20:31:11 hissy-re0 alarmd[555]: Alarm set: SFM color=RED, class=CHASSIS,
reason=No SFM Online, the box is not forwarding
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match sfm command to see error messages that are generated when an SFM fails or is offline. Use this information to diagnose a power supply problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display SFM Error Messages in the Chassis Daemon Log File

The chassis daemon (chassisd) log file keeps track of the state of each chassis component.

Action To display the SFM error messages logged in the chassis daemon log file, use the following CLI command:

user@host> **show log chassis | match sfm**

Sample Output

```
user@host> show log chassisd | match sfm
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x0
Jun 11 20:50:16 bp_handle_button_intr button status 0x0
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x8
Jun 11 20:50:16 bp_handle_button_intr button status 0x8
Jun 11 20:50:16 mcs_intr_handler fpm_mcsfd 10
Jun 11 20:50:16 mcs_intr mcs_ints_pending 0x7cbf20 button_status 0x8
Jun 11 20:50:16 bp_handle_button_intr button status 0x8
Jun 11 20:50:16 received second FPM key press, clearing timer!
Jun 11 20:50:18 bp_button_timer: taking sfm 1 offline
Jun 11 20:50:18 take_sfm_offline - slot 1 reason 7
Jun 11 20:50:18 cleaning up sfm 1 connection
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Blue LED Off [0x16]
Jun 11 20:50:18 SPP 1 - Blue LED Off
Jun 11 20:50:18 send: fpc 0, sfm 1 offline
Jun 11 20:50:18 send: fpc 1, sfm 1 offline
Jun 11 20:50:18 send: fpc 2, sfm 1 offline
Jun 11 20:50:18 send: fpc 6, sfm 1 offline
Jun 11 20:50:18 send: fpc 7, sfm 1 offline
Jun 11 20:50:18 fpc 2, sfm 1 offline ack
Jun 11 20:50:18 fpc 2, sfm 1 offline ack, online 0xc7 online-acks 0x4
Jun 11 20:50:18 fpc 1, sfm 1 offline ack
Jun 11 20:50:18 fpc 1, sfm 1 offline ack, online 0xc7 online-acks 0x6
Jun 11 20:50:18 fpc 0, sfm 1 offline ack
Jun 11 20:50:18 fpc 0, sfm 1 offline ack, online 0xc7 online-acks 0x7
```

```
Jun 11 20:50:18 fpc 7, sfm 1 offline ack
Jun 11 20:50:18 fpc 7, sfm 1 offline ack, online 0xc7 online-acks 0x87
Jun 11 20:50:18 fpc 6, sfm 1 offline ack
Jun 11 20:50:18 fpc 6, sfm 1 offline ack, online 0xc7 online-acks 0xc7
Jun 11 20:50:18 sfm_offline_now plane 1 conn 0x8152638
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert PLL Bypass [0x13]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert Board Reset [0x2e]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Assert ASIC Reset [0x28]
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Disable Power [0x10]
Jun 11 20:50:18 SPP 1 - Disable Power [addr 0x9 cmd 0x10]
Jun 11 20:50:18 CMB readback SPP 1 [0xe9, 0xf2] -> 0x26
Jun 11 20:50:18 power disable verified, SPP 1
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Blue LED Off [0x16]
Jun 11 20:50:18 SPP 1 - Blue LED Off
Jun 11 20:50:18 CMB cmd to SPP 1 [0xe9], Green LED Off [0x1a]
Jun 11 20:50:18 SPP 1 - Green LED Off
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Verifying SFM Failure

Steps To Take To verify SFM failure, follow these steps:

1. Check the SFM Connection on page 590
2. Restart the SFM on page 590
3. Perform an SFM Swap Test on page 591

Step 1: Check the SFM Connection

Action To check the SFM connection, make sure that it is properly seated in the midplane. Check the thumbscrews on the ejector locking tabs.

Step 2: Restart the SFM

Action To restart an SFM, use the following CLI command:

user@host> **request chassis sfm slot** *slot-number* **restart**

Sample Output For M40e routers:

```
user@host> request chassis sfm slot 0 restart
error: SFM 0 is transitioning to online state.
```

For M160 routers:

```
user@host> request chassis sfm slot 0 restart
Restart initiated, use "show chassis sfm" to verify
```

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Ready             0      0          0         0         0          0
  1  Online           38      1          0        64         8         46
  2  Offline        --- Unresponsive ---
  3  Online           39      1          0        64         8         46
```

What It Means The command output shows that the SFM restart has been initiated. On the M160 router, the command output indicates to use the show chassis sfm CLI command to verify that the SFM has been restarted. The SFM status information shows that the SFM is ready and that the status values are 0 for approximately 5 seconds until the SFM is active.

Step 3: Perform an SFM Swap Test

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SFM for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on an SFM, follow these steps:

1. Remove the chassis rear component cover by loosening the screws on the corners of the cover and pulling it straight out from the chassis.

2. Remove the SFM, as described in the M40e and M160 router hardware guides.

3. Take the SFM offline by using the request chassis sfm slot *slot-number* offline CLI command. You can also press and hold the offline button on the SFM faceplate at the rear of the router until the SFM OK LED turns off (about 5 seconds).

4. Replace the SFM with one that you know works.

5. Bring the SFM online. Press and hold the offline button on the SFM faceplate until the green OK LED lights (about 5 seconds). You can also use the request chassis sfm slot *slot-number* online CLI command.

6. Reinstall the rear component cover and tighten the screws to secure it to the chassis.

7. Check the SFM status. See "Display the SFM Summary Status" on page 582.

Controlling Redundant SFMs

Steps To Take To control the operation of an SFM, follow these steps:

Step 1: Take an SFM Offline

Action To take an SFM offline, use the following CLI command:

user@host> **request chassis sfm slot** *slot-number* **offline**

Sample Output

```
user@host> request chassis sfm slot 0 offline
Offline initiated, use "show chassis sfm" to verify
```

For M40e routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Offline        --- Offlined by cli command ---
  1  Online - Standby  41      4          0        64        16         46
```

For M160 routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online           41      3          0        64        17         46
  1  Online           44      4          0        64        17         46
  2  Online           44      4          0        64        17         46
  3  Offline        --- Offlined by cli command ---

Packet scheduling mode: Disabled
```

What It Means The sample output confirms that the SFM offline command has been initiated and specifies to use the show chassis sfm CLI command to verify that the SFM is offline. The command output for both the M40e and M160 routers shows that the SFM is offline and that this state was generated by running the CLI command.

Step 2: Bring an SFM Online

Action To bring an SFM online, use the following CLI command:

user@host> **request chassis sfm slot** *slot-number* **online**

Sample Output

```
user@host> request chassis sfm slot 0 online
Online initiated, use "show chassis sfm" to verify
```

For M40e routers:

```
user@host> show chassis sfm
Slot State           (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Present           0      0          0         0         0          0
  1  Online - Standby  41      4          0        64        16         46
```

For M160 routers:

```
user@host> show chassis sfm
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
  0  Online            41      3          0        64        17         46
  1  Online            44      3          0        64        17         46
  2  Online            44      3          0        64        17         46
  3  Present            0      0          0         0         0          0

Packet scheduling mode: Disabled
```

What It Means The sample output confirms that the SFM online command has been initiated and specifies to use the show chassis sfm CLI command to verify that the SFM is online. The command output shows that the SFM is present and that the values for the SFM status are 0 for approximately 5 seconds until the SFM is active.

Step 3: Switch SFM Mastership

Purpose You can switch SFM mastership on M40e routers only. By default, the SFM in slot 0 (SFM0) is the master and the SFM in slot 1 (SFM1) is the backup.

To change the default master SFM, include the sfm statement at the [edit chassis redundancy] hierarchy level in the configuration. For more information, see the *JUNOS System Basics Configuration Guide*.

Action To switch SFM mastership, use the following CLI command:

user@host> **request chassis sfm master switch** <**no-confirm**>

Sample Output

```
user@host> request chassis sfm master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between system forwarding module? [yes,no] (no) yes
Switch initiated, use “show chassis sfm” to verify
```

The following command output displays if you use the no-confirm option:

```
user@host> request chassis sfm master switch no-confirm
Switch initiated, use “show chassis sfm” to verify
```

Replacing an SFM

Action To replace an SFM, follow these steps:

1. Have ready an antistatic mat for the SFM.
2. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.
3. Remove the router rear component cover by loosening the screws on the corners of the cover and pulling it straight out from the chassis.
4. Press the offline button on the SFM faceplate and hold it down until the red FAIL LED lights (about 5 seconds).

5. Loosen the thumbscrews on the ejector locking tabs joining the two SFM boards.
6. Flip the ends of the ejector handles outward.
7. Grasp the handles, pull firmly on the SFM, and slide the unit about three-quarters of the way out of the chassis.
8. Move one of your hands underneath the SFM to support it, and slide it completely out of the chassis.
9. Hold the new SFM by placing one hand underneath to support it and the other hand on one of the ejector handles on the front of the unit.
10. Align the rear of the SFM with the guides inside the chassis.
11. Slide the unit completely into the chassis.
12. Press the ejector handles on the left and right sides of the SFM inward.
13. Tighten the thumbscrews on the ejector locking tabs.
14. Press the offline button on the SFM faceplate and hold it down until the green OK LED lights (about 5 seconds).
15. Reinstall the rear component cover and tighten the screws on the covers of the corner to secure it to the chassis.

Chapter 45

Monitoring Redundant PCGs

You monitor redundant Packet Forwarding Engine clock generators (PCGs) to ensure that a clocking signal is generated to synchronize the internal M40e and M160 router Packet Forwarding Engine components. (See Table 125.)

Table 125: Checklist for Monitoring Redundant PCGs

Monitor Redundant PCG Tasks	Command or Action
Understanding Redundant PCGs on page 596	
Displaying Redundant PCG Hardware Information on page 597	show chassis hardware
Monitoring Redundant PCG Status on page 597	
1. Monitor the Redundant PCG Environmental Status on page 597	show chassis environment show chassis environment pcg
2. Display the Redundant PCG Status from the Craft Interface on page 598	show chassis craft-interface
3. Check the PCG LED Status on the Faceplate on page 599	Remove the rear component cover and look on the PCG faceplate at the back of the M40e or M160 router chassis.
Determining Redundant PCG Mastership on page 599	
1. Display the PCG Master from the Craft Interface on page 599	show chassis craft-interface
2. Check the PCG LEDs on the Faceplate on page 600	Remove the rear component cover and look on the PCG faceplate at the rear of the M40e or M160 router chassis.
3. Display the Packet Forwarding Engine Current Clock Source on page 600	show chassis clocks
Displaying PCG Failure Alarms on page 600	show chassis alarms
Replacing a PCG on page 601	See "Return the Failed Component" on page 86, or follow the procedure in the M40e or M160 router hardware guide.
Bringing the Replaced PCG Online on page 602	request chassis pcg slot *slot-number* online
Verifying That the Replaced PCG Is Online on page 602	
1. Display the Replaced PCG Environmental Status on page 602	show chassis environment pcg
2. Display PCG Messages in the System Log File on page 603	show log messages | match PCG
3. Display PCG Error Messages in the Chassis Daemon Log File on page 603	show log chassisd | match PCG

See Also

- Monitoring the PCG on page 369

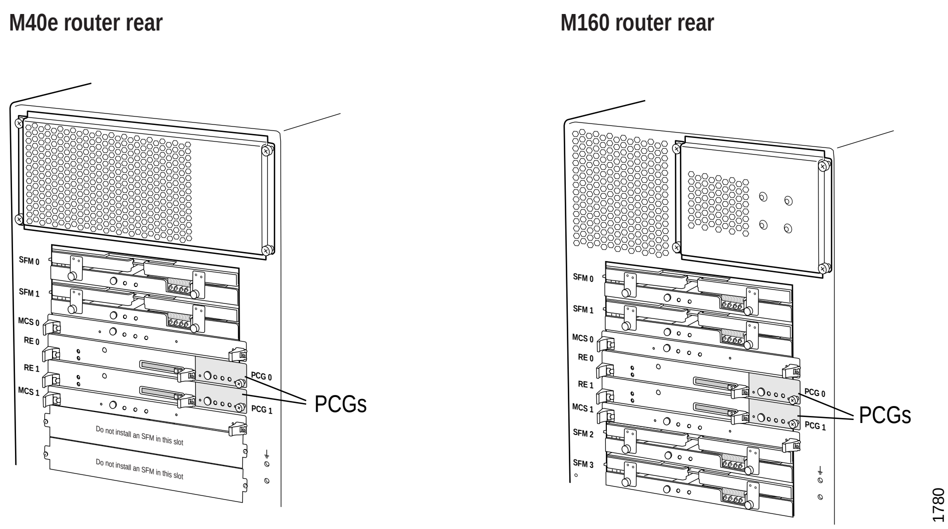
Understanding Redundant PCGs

Purpose You monitor redundant PCGs to ensure that they generate a clock signal to synchronize the modules and application-specific integrated circuits (ASICs) that make up the Packet Forwarding Engine.

What Are Redundant PCGs Redundant PCGs are two PCGs installed in a router. The PCG supplies a 125-MHz system clock to synchronize the modules and ASICs that make up the Packet Forwarding Engine.

The M40e and M160 routers have two PCGs located at the rear of the chassis in the slots labeled PCG0 and PCG1, to the right of the Routing Engine slots (see Figure 230).

Figure 230: M40e and M160 Router PCG Location



During normal operation, both PCGs generate a 125-MHz clock signal to the Packet Forwarding Engine modules, along with a signal indicating which is the master clock source. One PCG is designated as the master. The master Routing Engine controls which PCG is master and which is backup.

The modules and ASICs in the Packet Forwarding Engine that use the clock signal to gate packet processing use only the signal from the master PCG.

The PCGs are field-replaceable and hot-pluggable. You can remove and replace them without powering down the router, but the routing functions of the system are interrupted when a PCG is removed.

If the master PCG fails or you remove it from the chassis, the Packet Forwarding Engine resets so that the components start using the signal from the other PCG (which becomes the master). Packet forwarding halts while there is no clock signal because the Packet Forwarding Engine does not accept incoming packets. If the backup PCG fails or is removed, router function is not affected.

Displaying Redundant PCG Hardware Information

Action To display redundant PCG hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                20079             M160
Midplane         REV 03   710-001245   AB4132
FPM CMB          REV 02   710-001642   AB3264
FPM Display      REV 02   710-001647   AB3046
CIP              REV 04   710-001593   AB3284
PEM 0            Rev 03   740-001243   KM28409           DC
PEM 1            Rev 03   740-001243   KM13359           DC
PCG 0            REV 02   710-001568   AB3013
PCG 1            REV 02   710-001568   AB3000
[...Output truncated...]
```

What It Means The command output displays the PCG slot number, revision level, part number, and serial number.

Monitoring Redundant PCG Status

Steps To Take To monitor the PCG status, follow these steps:

1. Monitor the Redundant PCG Environmental Status on page 597
2. Display the Redundant PCG Status from the Craft Interface on page 598
3. Check the PCG LED Status on the Faceplate on page 599

Step 1: Monitor the Redundant PCG Environmental Status

Action To monitor the PCG environment status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                 Status     Measurement
Power PEM 0                OK
      PEM 1                OK
Temp  PCG 0                OK         41 degrees C / 105 degrees F
      PCG 1                OK         39 degrees C / 102 degrees F
[...Output truncated...]
```

What It Means The command output displays the slot number, status, and temperature of each PCG.

Alternative Action If there is a problem with the PCG status, you can display more detailed PCG environmental information with the following CLI command:

user@host> **show chassis environment pcg**

The command output is as follows:

```
PCG 0 status:
  State                           Online - PFE clock source
  Temperature                  41 degrees C / 105 degrees F
  Frequency:
    Setting                125.00 MHz
    Measurement            125.03 MHz
  Power:
    3.3 V                    3266 mV
    5.0 V bias               4981 mV
    8.0 V bias               8168 mV
  CMB Revision                 12
PCG 1 status:
  State                           Online
  Temperature                  39 degrees C / 102 degrees F
  Frequency:
    Setting                125.00 MHz
    Measurement            125.03 MHz
  Power:
    3.3 V                    3271 mV
    5.0 V bias               4971 mV
    8.0 V bias               8175 mV
  CMB Revision                 12
```

The command output displays the status for each PCG. The operating status can be Present, Online, Offline, or Empty. If Online, it can be the current PFE clock source (master) or backup. The command output displays the temperature of the air flowing past the PCG and the frequency setting and measurement for the PCG. The command output also displays information about the PCG power supplies and the revision level of the chassis management bus (CMB) slave.

Step 2: Display the Redundant PCG Status from the Craft Interface

Action To display the PCG LED states, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
PCG LEDs:
  PCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

[...Output truncated...]
```

What It Means The command output is for an M160 router. The PCGs in slots 0 and 1 are online and are functioning normally. The status colors represent the possible PCG operating states: Amber (Fail), Green (OK), and Blue (Master). The (*) indicates the current operating state.

Step 3: Check the PCG LED Status on the Faceplate

Action To check the PCG LEDs, remove the rear component cover and look on the PCG faceplate at the rear of the M40e or M160 router chassis.

Table 126 describes the functions of these LEDs.

Table 126: PCG LEDs

Color	Label	State	Description
Blue	MASTER	On steadily	PCG is master.
Green	OK	On steadily	PCG is operating normally.
		Blinking	PCG is starting up.
Amber	FAIL	On steadily	PCG has failed.

Determining Redundant PCG Mastership

If both PCGs are installed and functioning normally, PCG0 is the master and PCG1 is the backup by default.

Steps To Take To determine which PCG is operating as the master, follow these steps:

1. Display the PCG Master from the Craft Interface on page 599
2. Check the PCG LEDs on the Faceplate on page 600
3. Display the Packet Forwarding Engine Current Clock Source on page 600

Step 1: Display the PCG Master from the Craft Interface

Action To determine the PCG master from the craft interface status information, use the following CLI command:

user@host> **show chassis craft-interface**

Sample Output

```
user@host> show chassis craft-interface
[...Output truncated...]
PCG LEDs:
  PCG  0   1
--------------
Amber  .   .
Green  *   *
Blue   *   .

[...Output truncated...]
```

What It Means The command output shows that PCG0 is the master because the blue MASTER LED is on.

Step 2: Check the PCG LEDs on the Faceplate

Action To check the PCG LEDs, look on the PCG faceplate at the rear of the M40e or M160 router chassis. Table 126 on page 599 describes the PCG LED states. If the blue MASTER LED on the PCG faceplate is on steadily, the PCG is functioning as master.

Step 3: Display the Packet Forwarding Engine Current Clock Source

The Packet Forwarding Engine current clock source is the master PCG.

Action To display the PCG master from the Packet Forwarding Engine clock source output, use the following CLI command:

user@host> **show chassis clocks**

Sample Output

```
user@host> show chassis clocks
PFE clock status:
  Current source           PCG 0
  Measured frequency       125.03 MHz
Reference clock status:
  Current source           Primary
  Primary source           Internal
  Secondary source         Internal
  Tertiary source          Internal
  Rollover algorithm       Holdover
  PLL mode                 Free-running
  PLL errors               0
  Sync message current     0x00
  Sync message normal      0x00
  Sync message override    0x00
```

What It Means The command output shows that the PCG in slot 0 is the primary clock source or master.

Displaying PCG Failure Alarms

Action To display the current PCG alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
2 alarms currently active
Alarm time               Class  Description
2002-06-11 20:30:29 PDT  Minor PCG 0 Not Online
2002-06-11 20:30:32 PDT  Minor No PCGs Online
```

What It Means The command output displays the alarm date, time, severity level, and description.

Replacing a PCG

The PCGs are hot-pluggable. You can remove and replace them without powering down the router; however, the routing functions of the system are interrupted when the PCG is removed.

If both PCGs are installed and functioning normally, PCG0 is the master PCG and PCG1 is the backup by default.

Removing the backup PCG does not affect the functioning of the router. Taking the master PCG offline causes the Flexible PIC Concentrators (FPCs) and Switching and Forwarding Modules (SFMs) to power down and restart, with the other PCG selected as master. The forwarding and routing functions are interrupted during this process.

Action To remove and replace a PCG, follow these steps:

1. Lay an electrostatic bag or antistatic mat on a flat, stable surface to receive the PCG.
2. Attach an electrostatic discharge (ESD) strap to your bare wrist and connect the strap to one of the ESD points on the chassis.
3. Remove the rear component cover by loosening the screws at the corners of the cover and pulling it straight off of the chassis.
4. Press and hold the offline button on the PCG faceplate until the amber LED labeled FAIL lights, which takes about 3 seconds.

   If you are removing the master PCG, forwarding halts while the Packet Forwarding Engine resets so that the components start using the clock signal from the other PCG, which becomes the master.
5. Loosen the mounting screw on the right edge of the PCG faceplate, using a Phillips screwdriver if necessary.
6. Grasp the screw and slide the PCG about halfway out of the chassis.

CAUTION: Be careful to slide the PCG straight out of the chassis to avoid bending any of the pins on the underside of the board.

7. Place one hand under the PCG to support it, slide it completely out of the chassis, and place it on the antistatic mat or in the electrostatic bag.
8. Slide the PCG all the way into the card cage until it contacts the midplane.
9. Tighten the thumbscrew on the right side of the PCG faceplate.
10. Verify that the PCG is properly installed by looking at the LEDs on the PCG faceplate. The green OK LED should light steadily.
11. Reinstall the rear component cover and tighten the thumbscrews on the corners of the cover to secure it to the chassis.

Bringing the Replaced PCG Online

Action To bring the replaced PCG online, use the following CLI command:

user@host> **request chassis pcg slot** *slot-number* **online**

Sample Output

```
user@host> request chassis pcg slot 0 online
Online initiated, use ‘show chassis environment pcg” to verify
```

What It Means The PCG in slot 0 is brought online.

Verifying That the Replaced PCG Is Online

Steps To Take To verify that the replaced PCG is online, follow these steps:

1. Display the Replaced PCG Environmental Status on page 602
2. Display PCG Messages in the System Log File on page 603
3. Display PCG Error Messages in the Chassis Daemon Log File on page 603

Step 1: Display the Replaced PCG Environmental Status

Action To verify that the replaced PCG is online, use the following CLI command:

user@host> **show chassis environment pcg**

Sample Output

```
user@host> show chassis environment pcg
PCG 0 status:
   State                            Online
   Temperature                   30 degrees C / 86 degrees F
   Frequency:
     Setting                 125.00 MHz
     Measurement             125.01 MHz
   Power:
     3.3 V                     3278 mV
     5.0 V bias                4986 mV
     8.0 V bias                8222 mV
   CMB Revision                  12
PCG 1 status:
   State                            Online - PFE clock source
   Temperature                   43 degrees C / 109 degrees F
   Frequency:
     Setting                 125.00 MHz
     Measurement             124.95 MHz
   Power:
     3.3 V                     3269 mV
     5.0 V bias                4991 mV
     8.0 V bias                8222 mV
   CMB Revision                  12
```

What It Means When the replaced PCG is brought online, it does not automatically become master. It remains as the backup PCG until the master PCG fails, or you manually switch it to master by using the request chassis pcg online slot 1 CLI command.

Step 2: Display PCG Messages in the System Log File

Action To display the PCG error messages in the system log file to verify that a replaced PCG is online, use the following CLI command:

user@host> **show log messages | match PCG**

Sample Output

```
user@host> show log messages | match PCG
Aug 27 15:20:52 myrouter craftd[563]: Minor alarm cleared, PCG 0 Not Online
Aug 27 15:20:52 myrouter alarmd[562]: Alarm cleared: PCG color=YELLOW,
class=CHASSIS, reason=PCG 0 Not Online
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match pcg command to see error messages that are generated when a PCG fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display PCG Error Messages in the Chassis Daemon Log File

Action To display the PCG error messages in the chassis daemon (chassisd) log file and verify that a replaced PCG is online, use the following CLI command:

user@host> **show log chassisd | match PCG**

Sample Output

```
user@host> show log chassisd | match PCG
Aug 27 15:20:51 PCG 0 power verified on in 16 ms
Aug 27 15:20:52 reading PCG 0 initial state
Aug 27 15:20:52 CMB readback PCG 0 [0xe2, 0xff] -> 0xc
Aug 27 15:20:52 reading PCG 0 ideeprom
Aug 27 15:20:52 CMB cmd to PCG 0 [0xe2], Green LED On [0x1b]
Aug 27 15:20:52 PCG 0 - Green LED On
Aug 27 15:20:52 PCG 0 clear alarm 0x3
Aug 27 15:20:52 alarm op fru 1 op 0 reason 3
Aug 27 15:20:52 send: yellow alarm clear, class 100 obj 110 reason 3.
```

What It Means The chassisd database provides the date, time, and a component status message. The chassisd database is dynamic. It is initialized at router startup and is updated when components are added or removed.

Chapter 46

Monitoring Redundant SSBs

You monitor redundant M20 router System and Switch Boards (SSBs) to ensure that they do the following (see Table 127):

- Provide allocation of incoming data packets throughout shared memory on the Flexible PIC Concentrators (FPCs)
- Transfer outgoing data cells to the FPCs for packet reassembly
- Perform route lookups using the forwarding table, and monitor system components for failure and alarm conditions
- Monitor FPC operation and reset

Table 127: Checklist for Monitoring Redundant SSBs

Monitor Redundant SSB Tasks	Command or Action
Understanding Redundant SSBs on page 606	
Displaying Redundant SSB Configuration on page 608	configure show
Displaying Redundant SSB Hardware Information on page 608	show chassis hardware
Monitoring Redundant SSB Status on page 609	
1. Display the Redundant SSB Environmental Status on page 609	show chassis environment
2. Display the Redundant SSB Detailed Status on page 610	show chassis ssb *slot*
3. Check the Redundant SSB LEDs on page 610	Check the LEDs on the SSB faceplate.
Displaying Redundant SSB Mastership on page 611	
1. Display SSB Mastership from the Command Line on page 611	show chassis ssb
2. Check the SSB Mastership from the LEDs on page 612	Check the LEDs on the SSB panel of the craft interface.
Checking for SSB Alarms on page 612	
1. Display the Current SSB Alarms on page 612	show chassis alarms
2. Display SSB Error Messages in the System Log File on page 612	show log messages
3. Display SSB Error Messages in the Chassis Daemon Log File on page 613	show log chassisd

Monitor Redundant SSB Tasks	Command or Action
Verifying SSB Failure on page 613	
1. Check the SSB Connection on page 614	Check the thumbscrews on the left and right sides of the SSB.
2. Perform a Swap Test on the SSB on page 614	1. Take the SSB offline. 2. Remove the SSB. 3. Replace the SSB with one that you know works. 4. Verify that the new SSB works by using the show chassis ssb CLI command.
Switch SSB Mastership on page 615	request chassis ssb master switch <no-confirm>
Replacing the SSB on page 616	1. Take the SSB offline. 2. Remove the SSB. 3. Install a new SSB. 4. Verify that the new SSB works by using the show chassis ssb CLI command.

Understanding Redundant SSBs

Purpose Inspect redundant SSBs to ensure that they provide allocation of incoming data packets throughout shared memory on the FPCs, transfer outgoing data cells to the FPCs for packet reassembly, perform route lookups using the forwarding table, monitor system components for failure and alarm conditions, and monitor FPC operation and reset.

What Are Redundant SSBs SSBs are redundant when two SSBs are installed in the M20 router. The SSBs occupy the two top slots of the card cage (SSB0 and SSB1), and are installed into the midplane from the front of the chassis (see Figure 231 on page 607). By default, SSB0 is the master SSB and SSB1 is the backup. When the master SSB fails, automatic failover occurs and the backup SSB becomes the master. You can control which SSB is the master by including the ssb statement at the [edit chassis redundancy] hierarchy level in the configuration. For more information, see the *JUNOS System Basics Configuration Guide.*

The SSB performs the following major functions:

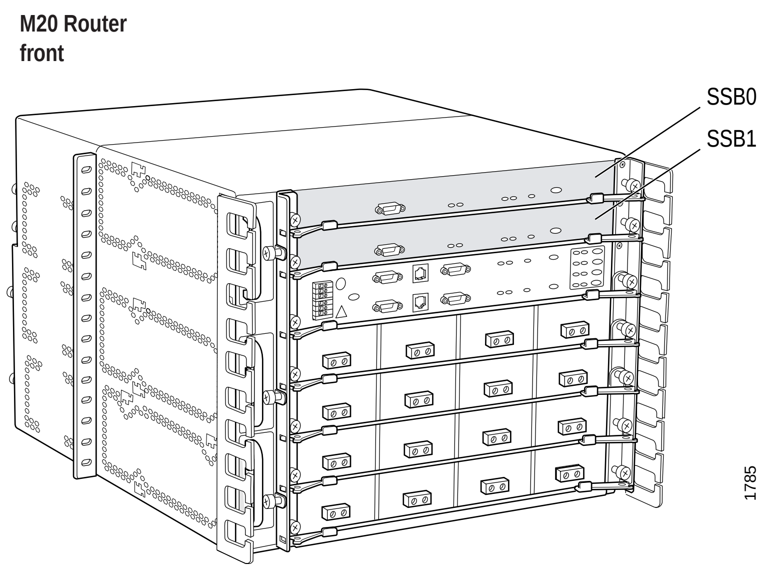
- Shared memory management on the FPCs—The Distributed Buffer Manager application-specific integrated circuit (ASIC) on the SSB uniformly allocates incoming data packets throughout shared memory on the FPCs.
- Outgoing data cell transfer to the FPCs—A second Distributed Buffer Manager ASIC on the SSB passes data cells to the FPCs for packet reassembly when the data is ready to be transmitted.
- Route lookups—The Internet Processor ASIC on the SSB performs route lookups using the forwarding table stored in synchronous SRAM (SSRAM). After performing the lookup, the Internet Processor ASIC informs the midplane of the forwarding decision, and the midplane forwards the decision to the appropriate outgoing interface.

- System component monitoring—The SSB monitors other system components for failure and alarm conditions. It collects statistics from all sensors in the system and relays them to the Routing Engine, which sets the appropriate alarm. For example, if a temperature sensor exceeds the first internally defined threshold, the Routing Engine issues a "high temp" alarm. If the sensor exceeds the second threshold, the Routing Engine initiates a system shutdown.

- Exception and control packet transfer—The Internet Processor ASIC passes exception packets to a microprocessor on the SSB, which processes almost all of them. The remaining packets are sent to the Routing Engine for further processing. Any errors that originate in the Packet Forwarding Engine and are detected by the SSB are sent to the Routing Engine using system log messages.

- FPC reset control—The SSB monitors the operation of the FPCs. If it detects errors in an FPC, the SSB attempts to reset the FPC. After three unsuccessful resets, the SSB takes the FPC offline and informs the Routing Engine. Other FPCs are unaffected, and normal system operation continues.

Figure 231: M20 Router Redundant SSB Location



The SSB houses the Internet Processor ASIC and two Distributed Buffer Manager ASICs.

The SSB is hot-pluggable. You can remove and replace it without powering down the system; however this causes major impact to the system. The following functions cannot occur while the SSB is removed from the router:

- Route lookups

- System component monitoring

- Exception and control packet monitoring

- FPC resets

When you remove the SSB, all packet forwarding stops immediately and the Routing Engine responds by generating alarms. When you replace the SSB, it is rebooted by flash EEPROM.

If you remove the Routing Engine, the SSB enters a warm shutdown mode and continues its forwarding process for a limited time using a frozen forwarding table. The time limit is determined by a timer in the SSB. If you replace the Routing Engine during the warm shutdown period, the SSB unfreezes its forwarding tables and resumes normal functioning. Otherwise, the SSB shuts itself down.

Displaying Redundant SSB Configuration

You can configure which SSB is the master and which is the backup. By default, the SSB in slot 0 is the master and the SSB in slot 1 is the backup. You can modify the default configuration by including the ssb statement at the [edit chassis redundancy] hierarchy level.

NOTE: We recommend that both Routing Engines have the same configuration.

To display the current SFM redundancy configuration, follow these steps:

1. Enter the CLI configuration mode using the following command:

   user@host# **configure**

2. Go to the [edit chassis redundancy] hierarchy level.

3. Show the SFM configuration using the following command:

   user@host# **show**

Displaying Redundant SSB Hardware Information

Action To display the SSB hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
[...Output truncated...]
SSB slot 0       REV 01   710-001951   AD5904            Internet Processor II
SSB slot 1       N/A      N/A          N/A               backup
[...Output truncated...]
```

What It Means The command output displays the SSB version level, part number, serial number, and description.

Monitoring Redundant SSB Status

Steps To Take To monitor the SSB, follow these steps:

1. Display the Redundant SSB Environmental Status on page 609
2. Display the Redundant SSB Detailed Status on page 610
3. Check the Redundant SSB LEDs on page 610

Step 1: Display the Redundant SSB Environmental Status

Action To display the SSB environmental status, use the following CLI command:

user@host> **show chassis environment**

Sample Output

```
user@host> show chassis environment
Class Item                   Status     Measurement
Power Power Supply A         Failed
      Power Supply B         OK
Temp  FPC Slot 0             OK         27 degrees C / 80 degrees F
      FPC Slot 1             OK         30 degrees C / 86 degrees F
      FPC Slot 2             OK         26 degrees C / 78 degrees F
      FPC Slot 3             OK         25 degrees C / 77 degrees F
      Power Supply A         OK         28 degrees C / 82 degrees F
      Power Supply B         OK         24 degrees C / 75 degrees F
      SSB Slot 0             OK         25 degrees C / 77 degrees F
      Backplane              OK         21 degrees C / 69 degrees F
Fans  Rear Fan               OK         Spinning at normal speed
      Upper Fan              OK         Spinning at normal speed
      Middle Fan             OK         Spinning at normal speed
      Bottom Fan             OK         Spinning at normal speed
Misc  Craft Interface        OK
```

What It Means The command output displays the SSB status and temperature. The SSB status can be OK, Failed, or Absent.

Step 2: Display the Redundant SSB Detailed Status

Action To display more detailed SSB status information, use the following CLI command:

user@host> **show chassis ssb**

Sample Output

```
user@host> show chassis ssb
SSB status:
  Failover:                      0 time
  Slot 0:
    State:                         Master
    Temperature:                33 Centigrade
    CPU utilization:             0 percent
    Interrupt utilization:       0 percent
    Heap utilization:            0 percent
    Buffer utilization:          6 percent
    DRAM:                       64 Mbytes
    Start time:                    1999-01-15 22:05:36 UTC
    Uptime:                        21 hours, 21 minutes, 22 seconds
  Slot 1:
    State:                         Backup
```

What It Means The command output displays the number of times the mastership has changed, the SSB slot number 0 or 1, and the current state of the SSB: Master, Backup, or Empty. The command output displays the temperature of the air passing by the SSB, in degrees Centigrade. It also displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the SSB processor, including the total DRAM available to the SSB processor. The command output displays the time when the SSB started running and how long it has been running.

Alternative Action To display the status for a particular SSB, use the following CLI command:

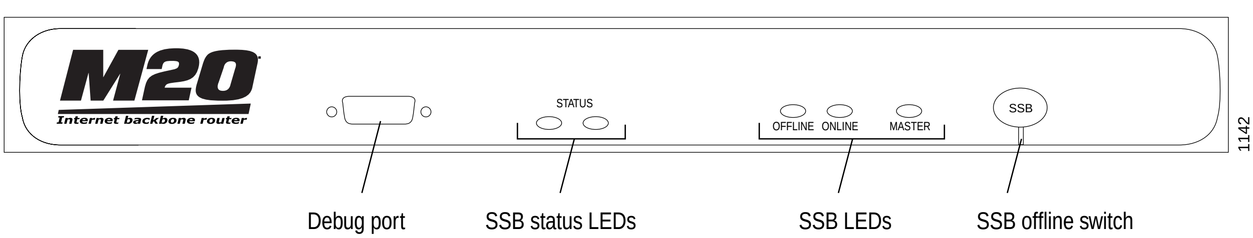
user@host> **show chassis ssb** *slot*

Step 3: Check the Redundant SSB LEDs

Periodically check the SSB LEDs to verify that the SSB is online or offline and the type of task it is performing.

Action To check the SSB LEDs, look on the faceplate at the front of the router (see Figure 232).

Figure 232: SSB LEDs



The SSB has two groups of LEDs: online/offline LEDs and status LEDs. The online/offline LEDs indicate whether the SSB is online or offline. The status LEDs indicate what type of task the SSB is performing. Table 128 describes the SSB LEDs.

Table 128: SSB LED States

Label	Color	State	Description
OFFLINE	Amber	On steadily	SSB is offline.
ONLINE	Green	On steadily	SSB processor is running.
MASTER	Blue	On steadily	SSB is master.
STATUS (left)	Green	Blinking	SSB processor is running. Normally, the blinking is faint and becomes bright only when the SSB is processing many exceptions.
STATUS (right)	Green	Flashing	I/O interrupts are occurring.

Displaying Redundant SSB Mastership

Steps To Take To display the SSB mastership information, follow these steps:

1. Display SSB Mastership from the Command Line on page 611
2. Check the SSB Mastership from the LEDs on page 612

Step 1: Display SSB Mastership from the Command Line

Action To display more detailed SSB status information, use the following CLI command:

user@host> **show chassis ssb**

Sample Output

```
user@host> show chassis ssb
SSB status:
  Failover:                     0 time
  Slot 0:
    State:                        Master
    Temperature:               33 Centigrade
    CPU utilization:            0 percent
    Interrupt utilization:      0 percent
    Heap utilization:           0 percent
    Buffer utilization:         6 percent
    DRAM:                      64 Mbytes
    Start time:                   1999-01-15 22:05:36 UTC
    Uptime:                       21 hours, 21 minutes, 22 seconds
  Slot 1:
    State:                        Backup
```

What It Means The command output displays the number of times the mastership has changed, the SSB slot number 0 or 1, and the current state of the SSB: Master, Backup, or Empty. The command output displays the temperature of the air passing by the SSB, in degrees Centigrade. It also displays the total percentage of CPU, interrupt, heap space, and buffer space being used by the SSB processor, including the total DRAM available to the SSB processor. The command output displays the time when the SSB started running and how long it has been running.

Step 2: Check the SSB Mastership from the LEDs

Action To check the SSB mastership from the LEDs, look on the faceplate at the front of the router (see Figure 232 on page 610).

The SSB has two groups of LEDs: online/offline LEDs and status LEDs. The online/offline LEDs indicate whether the SSB is online or offline. The status LEDs indicate what type of task the SSB is performing. Table 128 on page 611 describes the SSB LEDs.

Checking for SSB Alarms

Steps To Take To check for SSB alarms, follow these steps:

1. Display the Current SSB Alarms on page 612
2. Display SSB Error Messages in the System Log File on page 612
3. Display SSB Error Messages in the Chassis Daemon Log File on page 613

Step 1: Display the Current SSB Alarms

Action To display the current SSB alarms, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
2 alarms currently active
Alarm time               Class  Description
2002-06-05 19:55:57 UTC  Major  fxp0: ethernet link down
```

What It Means The command output displays the alarm date, time, severity level, and description. An SSB failure or removal generates an fxp0 link alarm. The fxp0 link is the dedicated 100-Mbps Fast Ethernet link between the SSB and the Routing Engine. This link transfers routing table data from the Routing Engine to the forwarding table in the Internet Processor ASIC. The link also transfers, from the SSB to the Routing Engine, routing link-state updates and other packets destined for the router that have been received through the router interfaces.

Step 2: Display SSB Error Messages in the System Log File

Periodically check the system log messages on the management console for messages sent by the SSB. During normal operation, the SSB notifies the Routing Engine of any errors it detects.

Action To display the SSB error messages in the system log file, use the following CLI command:

user@host> **show log messages**

Sample Output

```
user@host> show log messages
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 100Mb / full-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 10Mb / half-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: media DOWN 100Mb / full-duplex
Jul 10 13:28:45 myrouter /kernel: fxp1: link UP 100Mb / full-duplex
Jul 10 13:28:45 myrouter rpd[564]: EVENT <UpDown> fxp1.0 index 1 <Up Broadcast
Multicast> address #0 0.a0.a5.12.1d.6d
Jul 10 13:28:45 myrouter mib2d[563]: SNMP_TRAP_LINK_UP: ifIndex 2, ifAdminStatus
up(1), ifOperStatus up(1), ifName fxp1
[...Output truncated...]
```

What It Means The messages system log file records the time the failure or event occurred, the severity level, a code, and a message description. You can also use the show log messages | match ssb command to see error messages that are generated when an SSB fails or is offline. Use this information to diagnose a problem and to let the Juniper Networks Technical Assistance Center (JTAC) know what error messages were generated and the router events that occurred before and after the problem. For more information about system log messages, see the *JUNOS System Log Messages Reference*.

Step 3: Display SSB Error Messages in the Chassis Daemon Log File

Action To display the SSB error messages in the chassis daemon (chassisd) log file, use the following CLI command:

user@host> **show log chassisd**

Sample Output

```
user@host> show log chassisd
Jul 10 13:27:28 SSB0 is now not present
Jul 10 13:27:28 Assert reset on SSB0
Jul 10 13:27:28 Turn on ethernet loop
[...Output truncated...]
```

What It Means The command output displays the SSB hardware version level, part number, and serial number.

Verifying SSB Failure

Steps To Take To verify SSB failure, follow these steps:

1. Check the SSB Connection on page 614
2. Perform a Swap Test on the SSB on page 614

Step 1: Check the SSB Connection

If the SSB is not seated properly, it will not function.

Action To check the SSB connection, make sure that the SSB is properly seated in the slot. To seat the SSB properly adequately, tighten the screws on the left and right sides of the card carrier.

Step 2: Perform a Swap Test on the SSB

CAUTION: Before performing a swap test, always check for bent pins in the midplane and check the SCB for stuck pins in the connector. Pins stuck in the component connector can damage other good slots during a swap test.

Action To perform a swap test on the SSB, follow these steps:

1. Attach an electrostatic discharge (ESD) wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.

2. Locate the SSB offline switch on the front panel and press and hold the switch for 5 seconds to take the SSB offline.

CAUTION: If you take the SSB offline, packet forwarding will be affected.

3. Unscrew the thumbscrews on the left and right sides of the card carrier to unseat the SSB from the midplane.

4. Flip the ends of the two extractor clips, which are adjacent to the thumbscrews, towards the outside edges of the router.

5. Grasp both sides of the card carrier and slide the SSB about three-quarters of the way out of the router.

6. Move one of your hands underneath the SSB to support it, and slide it completely out of the chassis.

7. Replace the SSB with one that you know works.

8. Grasp the front of the SSB card carrier with both hands and align the back of the card carrier with the slide guides on the chassis.

9. Slide the SSB card carrier all the way into the card cage until it contacts the midplane.

10. Flip the extractor clips, located on the left and right sides of the card carrier, towards each other to secure the SSB in place.

11. Tighten the thumbscrews on the left and right sides of the card carrier to seat the SSB.

NOTE: To seat the SSB properly, be sure to tighten the screws adequately. If the SSB is not seated properly, it will not function.

12. Verify that the SSB works by using the show chassis ssb CLI command. (See “Display the Redundant SSB Detailed Status” on page 610.)

Switch SSB Mastership

Purpose To change the default master SSB, include the ssb statement at the [edit chassis redundancy] hierarchy level in the configuration. For more information, see the *JUNOS System Basics Configuration Guide*.

Action To control which SSB is master, use the following CLI command:

user@host> **request chassis ssb master switch <no-confirm>**

Sample Output

```
user@host> request chassis ssb master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between system switch boards ? [yes,no] (no) yes
Switch initiated, use “show chassis ssb” to verify
```

If you use the no-confirm option, the command output is as follows:

```
user@host> request chassis ssb master switch no-confirm
Switch initiated, use “show chassis ssb” to verify
```

What It Means By default, the SSB in slot 0 (SSB0) is the master and the SSB in slot 1 (SSB1) is the backup.

NOTE: For routers that have two SSBs, both SSBs must be running JUNOS Release 4.0 or later. Do not run JUNOS Release 3.4 on one of the SSBs and JUNOS Release 4.0 or later on the other.

JUNOS Release 3.4 does not support SSB redundancy; if you are using this release of the software, only one SSB can be installed in the router. It can be installed in either slot.

The configurations on the two SSBs do not have to be the same, and they are not automatically synchronized. If you configure both SSBs as masters, when the chassis software restarts for any reason, the SSB in slot 0 becomes the master and the SSB in slot 1 becomes the backup.

Replacing the SSB

Purpose The SSB is hot-pluggable. When the SSB is removed, all packet forwarding stops immediately and the Routing Engine responds by sending alarms through the Ethernet channel to the management console. When the SSB is replaced, it is rebooted by flash EEPROM.

Action To replace a failed SSB, follow these steps:

1. Attach an ESD wrist strap to your bare wrist, and connect the wrist strap to one of the two ESD points on the chassis.

2. Locate the SSB offline switch on the front panel and press and hold the switch for 5 seconds to take the SSB offline.

CAUTION: If you take the SSB offline, packet forwarding will be affected.

3. Unscrew the thumbscrews on the left and right sides of the card carrier to unseat the SSB from the midplane.

4. Flip the ends of the two extractor clips, which are adjacent to the thumbscrews, towards the outside edges of the router.

5. Grasp both sides of the card carrier and slide the SSB about three-quarters of the way out of the router.

6. Move one of your hands underneath the SSB to support it, and slide it completely out of the chassis.

7. Replace the SSB with one that you know works.

8. Grasp the front of the SSB card carrier with both hands and align the back of the card carrier with the slide guides on the chassis.

9. Slide the SSB card carrier all the way into the card cage until it contacts the midplane.

10. Flip the extractor clips, located on the left and right sides of the card carrier, towards each other to secure the SSB in place.

11. Tighten the thumbscrews on the left and right sides of the card carrier to seat the SSB.

NOTE: To seat the SSB properly, be sure to tighten the screws adequately. If the SSB is not seated properly, it will not function.

12. Verify that the SSB works by using the show chassis ssb CLI command. (See "Display the Redundant SSB Detailed Status" on page 610.)

Chapter 47

Monitoring Redundant CFEBs

You monitor redundant Compact Forwarding Engine Boards (CFEBs) in the M10i router. A CFEB provides route lookup, filtering, and switching on incoming data packets, then directs outbound packets to the appropriate interface for transmission to the network. (See Table 129.)

The M10i router CFEB can process 16 million packets per second (Mpps).

The CFEB communicates with the Routing Engine using a dedicated 100-Mbps Fast Ethernet link that transfers routing table data from the Routing Engine to the forwarding table in the integrated ASIC. The link is also used to transfer from the CFEB to the Routing Engine routing link-state updates and other packets destined for the router that have been received through the router interfaces.

Table 129: Checklist for Monitoring the CFEB

Monitor CFEB Tasks	Command or Action
Understanding Redundant CFEBs on page 618	
Displaying Redundant CFEB Hardware Information on page 620	show chassis hardware
Displaying CFEB Mastership on page 620	
1. Check CFEB LEDs on page 620	Look at the LEDs on the CFEB faceplate located on the rear of the router above the power supplies.
2. Display the CFEB Status on page 621	show chassis cfeb
Display CFEB Alarms on page 621	See "Checking for CFEB Alarms" on page 423. For conditions that trigger CFEB alarms, see "Display the Current Router Alarms" on page 61.
Verifying CFEB Failure on page 621	See "Verifying CFEB Failure" on page 621.
Returning the CFEB on page 621	See "Return the Failed Component" on page 86 or follow the procedure in the appropriate hardware guide.

Understanding Redundant CFEBs

Purpose

Monitor redundant CFEBs so they can provide route lookup, filtering, and switching on incoming data packets and direct outbound packets to the appropriate interface for transmission to the network.

What Are Redundant CFEBs

Two CFEBs are installed in the M10i router. The M10i router CFEB processes 16 Mpps.

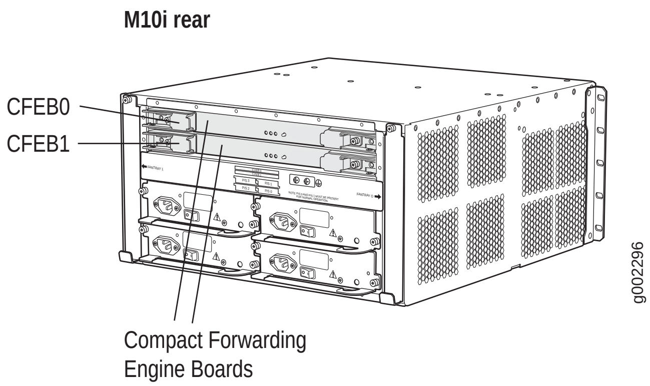
The CFEB performs the following functions:

- Route lookups—Performs route lookups using the forwarding table stored in the synchronous SRAM (SSRAM).
- Shared memory management—Uniformly allocates incoming data packets throughout the router's shared memory.
- Outgoing data packets transfer—Passes data packets to the destination FIC or PIC when the data is ready to be transmitted.
- Exception and control packet transfer—Passes exception packets to the microprocessor on the CFEB, which processes almost all of them. The rest are sent to the Routing Engine for further processing. Any errors originating in the Packet Forwarding Engine and detected by the CFEB are sent to the Routing Engine using system log messages.
- (M7i router only) Built-in tunnel interface—Encapsulates arbitrary packets inside a transport protocol, providing a private, secure path through an otherwise public network.

  The built-in tunnel interface on the CFEB is configured the same way as a PIC. For information about configuring the built-in tunnel interface, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.
- (M7i router only) Optional Adaptive Services PIC–Integrated (ASP–I)—Provides one or more services on one PIC. See "Adaptive Services PIC–Integrated (ASP–I)" on page 11 for more information.

One or two CFEBs can be installed into the midplane from the rear of the chassis, as shown in Figure 233 on page 619. Only one CFEB is active at a time; the optional second CFEB is in standby mode. By default, the CFEB in slot CFEB 0 is active. To modify the default, include the appropriate cfeb statement at the [edit chassis redundancy] hierarchy level of the configuration, as described in the section about CFEB redundancy in the *JUNOS System Basics Configuration Guide*.

Figure 233: M10i Router CFEB Location



CFEBs are hot-pluggable. Removing the standby CFEB has no effect on router function. If the active CFEB fails or is removed from the chassis, the effect depends on how many CFEBs are installed:

- If there is one CFEB, forwarding halts until the CFEB is replaced and functioning again. It takes approximately one minute for the replaced CFEB to boot and become active. Reading in router configuration information can take additional time, depending on the complexity of the configuration.
- If there are two CFEBs, forwarding halts while the standby CFEB boots and becomes active, which takes approximately one minute. Synchronizing router configuration information can take additional time, depending on the complexity of the configuration.

See Also

- Host Redundancy Overview on page 463
- Monitoring the CFEBs on page 417
- Monitoring Redundant CFEBs on page 617
- Monitoring the Routing Engine on page 125
- Monitoring Redundant Routing Engines on page 491

Displaying Redundant CFEB Hardware Information

Action To view redundant CFEB hardware information, use the following command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                31655             M10i
Midplane         REV 04   710-008920   CD7925            M10i Midplane
Power Supply 0   Rev 05   740-008537   QE16399           AC Power Supply
Power Supply 1   Rev 05   740-008537   QF11145           AC Power Supply
HCM slot 0       REV 01   710-010580   CE1729            M10i HCM
HCM slot 1       REV 01   710-010580   CE1769            M10i HCM
Routing Engine 0 REV 00   740-011202   1000525660        RE-850
Routing Engine 1 REV 00   740-011202   1000540499        RE-850
CFEB slot 0      REV 03   750-010465   CC7348            Internet Processor II
CFEB slot 1      REV 03   750-010470   CC7350            Backup
[...Output truncated...]
```

What It Means The command output shows that two CFEBs are installed in the M10i router. The command output also displays the CFEB version level, part number, serial number, and description.

Displaying CFEB Mastership

Steps To Take To display CFEB mastership, follow these steps:

1. Check CFEB LEDs on page 620
2. Display the CFEB Status on page 621

Step 1: Check CFEB LEDs

Three LEDs—a green LED labeled OK, a red LED labeled FAIL, and a blue LED labeled MASTER—indicate CFEB status.

Action Look at the LEDs on the CFEB faceplate. The CFEB is located on the rear of the router above the power supplies (see Figure 233 on page 619). Table 130 describes the CFEB LED states.

Table 130: CFEB LEDs

Label	Color	State	Description
OK	Green	On steadily	CFEB is running normally.
		Blinking	CFEB is starting up.
FAIL	Red	On steadily	CFEB is not operational or is in reset mode.
MASTER	Blue	On steadily	CFEB is functioning as master.

Step 2: Display the CFEB Status

Action To display CFEB status to show mastership, use the following CLI command:

user@host> **show chassis cfeb**

Sample Output

```
user@host> show chassis cfeb
CFEB status:
Slot 0 information:
  State                                 Master
  Intake temperature                 29 degrees C / 84 degrees F
  Exhaust temperature                38 degrees C / 100 degrees F
  CPU utilization                     3 percent
  Interrupt utilization               0 percent
  Heap utilization                   10 percent
  Buffer utilization                 22 percent
  Total CPU DRAM                    128 MB
  Internet Processor II                 Version 1, Foundry IBM, Part number 164
  Start time:                           2004-09-28 03:07:54 PDT
  Uptime:                             9 days, 18 hours, 36 minutes, 15 seconds
Slot 1 information:
  State                                 Backup
  Intake temperature                 29 degrees C / 84 degrees F
  Exhaust temperature                38 degrees C / 100 degrees F
  CPU utilization                     3 percent
  Interrupt utilization               0 percent
  Heap utilization                   10 percent
  Buffer utilization                 22 percent
  Total CPU DRAM                    128 MB
  Internet Processor II                 Version 1, Foundry IBM, Part number 164
  Start time:                           2004-09-28 03:07:54 PDT
  Uptime:                             9 days, 18 hours, 36 minutes, 15 seconds
```

What It Means The command output displays which CFEB is master and backup, as well as other environmental and memory information.

Display CFEB Alarms

Action To display CFEB alarms, see "Checking for CFEB Alarms" on page 423. For conditions that trigger CFEB alarms, see "Display the Current Router Alarms" on page 61.

Verifying CFEB Failure

Action To verify CFEB failure, see "Verifying CFEB Failure" on page 621.

Returning the CFEB

Action To replace the CFEB, see "Return the Failed Component" on page 86, or follow the procedure in the *M10i Internet Router Hardware Guide*.

Chapter 48

Monitoring Redundant HCMs

You monitor redundant High-Availability Chassis Managers (HCMs) on the M10i router so they can work with a companion Routing Engine to provide control and monitoring functions for router components. The HCMs also display alarm status and take Physical Interface Cards (PICs) online and offline.

Table 131 provides a checklist of tasks for you to perform to monitor redundant HCMs.

Table 131: Checklist for Monitoring Redundant HCMs

Monitor Redundant HCM Tasks	Command or Action
Understanding Redundant HCMs on page 624	
Displaying Redundant HCM Hardware Information on page 625	show chassis hardware
Displaying HCM Status and Mastership on page 625	
1. Check the HCM LEDs on page 625	Look at the LEDs on the HCM faceplate. The master HCM LED light flashes blue.
2. Check the HCM Environmental Status on page 626	show chassis environment hcm
Switching HCM Mastership on page 627	request chassis routing-engine master switch
Displaying HCM Alarms on page 628	show chassis alarms
Performing a Swap Test on an HCM on page 629	See “Performing A Swap Test” on page 438.
Returning an HCM on page 629	Find the serial number ID label, then see “Return the Failed Component” on page 86. See also the *M10i Internet Router Hardware Guide*.

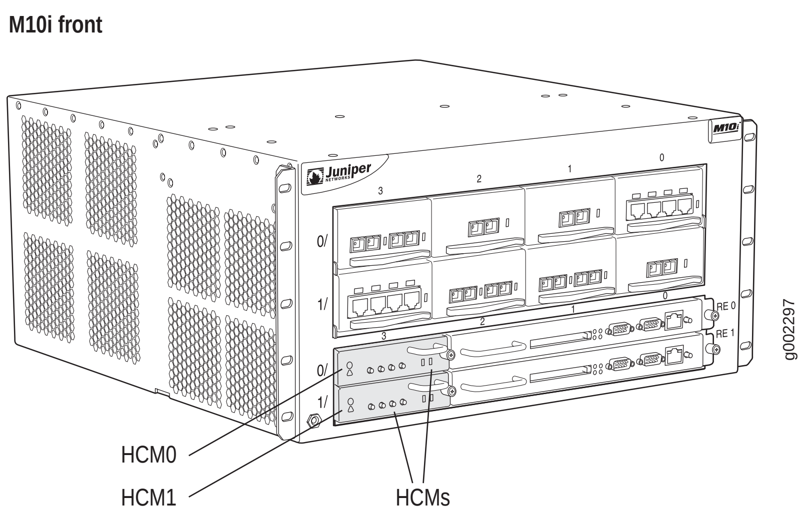
Understanding Redundant HCMs

Purpose You monitor and maintain HCMs on the M10i router so that they can monitor and control router components, control component power-up and power-down, signal which Routing Engine is master, display alarm conditions, and take PICs offline.

What Are Redundant HCMs Two HCMs are installed in an M10i router. Each HCM works with a companion Routing Engine.

Two HCMs are installed into the midplane from the front of the chassis, as shown in Figure 234. The master HCM performs all functions and provides PIC removal buttons for the first Flexible PIC Concentrator (FPC). The standby HCM provides PIC removal buttons for the second FPC. The HCM in the slot labeled HCM0 is paired with the Routing Engine in the slot labeled RE0. Likewise, the HCM in the slot labeled HCM1 is paired with the Routing Engine in the slot labeled RE1. By default, the HCM in the slot labeled HCM0 is the master.

Figure 234: Redundant HCMs



When HCM mastership changes because of failure, Routing Engine mastership also changes.

The HCM is hot-pluggable.

See Also
- M10i Internet Router Overview on page 11
- Monitoring the HCM on page 431
- Host Redundancy Overview on page 463
- Monitoring Redundant Routing Engines on page 491

Displaying Redundant HCM Hardware Information

Action To display the redundant HCM hardware information, use the following JUNOS software command-line interface (CLI) command:

user@host> **show chassis hardware**

Sample Output

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                31875             M10i
Midplane         REV 04   710-008920   CE1044            M10i Midplane
Power Supply 0   Rev 05   740-008537   QE16425           AC Power Supply
Power Supply 1   Rev 05   740-008537   QE16644           AC Power Supply
HCM slot 0       REV 01   710-010580   CC7625            M10i HCM
HCM slot 1       REV 01   710-010580   CC7629            M10i HCM
Routing Engine 0 REV 09   740-009459   1000513670        RE-5.0
Routing Engine 1 REV 09   740-009459   1000513630        RE-5.0
```

What it Means The command output shows that on this M10i router, two HCMs are installed in slots 0 (HCM0) and 1 (HCM1) along with their companion Routing Engines. By default, the HCM in the slot labeled HCM0 is the master.

Displaying HCM Status and Mastership

By default, the HCM in the slot labeled HCM0 is the master.

Steps To Take To display the redundant HCM status and mastership, follow these steps:

1. Check the HCM LEDs on page 625
2. Check the HCM Environmental Status on page 626

Step 1: Check the HCM LEDs

Action To see which HCM is functioning as master, look at the LEDs on the HCM faceplate. On the HCM faceplate, two LEDs indicate HCM status—a green PWR LED and a blue MSTR LED. Table 132 describes the LED states.

Table 132: HCM LEDs

Label	Color	State	Description
PWR	Green	On steadily	HCM is functioning normally.
		Blinking	HCM is starting up.
MSTR	Blue	On steadily	HCM is master.

Step 2: Check the HCM Environmental Status

Action To check the HCM environmental status and view which HCM is functioning as master, use the following CLI command:

user@host> **show chassis environment hcm**

Sample Output

```
user@host> show chassis environment hcm
HCM 0 status:
  State                           Online Master
  FPGA Revision                27
HCM 1 status:
  State                           Online Standby
  FPGA Revision                27
```

What it Means The command output shows that both HCMs (HCM0 and HCM1) are online. HCM0 is functioning as master, and HCM1 is functioning as standby. The command output also gives the Field Programmable Gate Array (FPGA) revision level. The FPGA is a gate on the chip used in the HCM.

Alternative Action To display the status of an HCM in a certain slot, use the following CLI command:

user@host> **show chassis environment hcm 1**

Sample Output

```
user@host> show chassis environment hcm 1
HCM 1 status:
  State                           Online Standby
  FPGA Revision                27
```

Switching HCM Mastership

When HCM mastership changes because of failure, Routing Engine mastership will change as well.

If the Routing Engines are running JUNOS Release 6.0 or later and are configured for graceful switchover, the standby Routing Engine immediately assumes Routing Engine functions and there is no interruption to packet forwarding. Otherwise, packet forwarding halts while the standby Routing Engine becomes the master and the Packet Forwarding Engine components reset and connect to the new master Routing Engine. For information about configuring graceful switchover, see the section about Routing Engine redundancy in the *JUNOS System Basics Configuration Guide.*

NOTE: Router performance might change if the standby Routing Engine's configuration differs from the former master's configuration. For the most predictable performance, configure the two Routing Engines identically, except for parameters unique to a Routing Engine, such as the hostname defined at the [edit system] hierarchy level and the management interface (fxp0 or equivalent) defined at the [edit interfaces] hierarchy level.

To configure Routing Engine-specific parameters and still use the same configuration on both Routing Engines, include the appropriate configuration statements under the re0 and re1 statements at the [edit groups] hierarchy level and use the apply-groups statement. For instructions, see the *JUNOS System Basics Configuration Guide.*

Action To switch HCM mastership to the backup HCM, use the following CLI command:

user@host> **request chassis routing-engine master switch**

Sample Output

```
user@host> request chassis routing-engine master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between routing engines ? [yes,no] yes

Resolving mastership...
Complete. The other routing engine becomes the master.
```

What It Means The HCM that was master is now the backup HCM.

Action To check HCM status and mastership after a switchover, use the following CLI command:

user@host> **show chassis environment hcm**

Sample Output

```
user@host> show chassis environment hcm
HCM 0 status:
  State                          Online Standby
  FPGA Revision               27
HCM 1 status:
  State                          Online Master
  FPGA Revision               27
```

Action To switch HCM mastership from the backup to the default master, use the following CLI command

```
user@host> request chassis routing-engine master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between routing engines ? [yes,no] (no) yes

Resolving mastership...

Message from syslogd@host cfeb at Jan 28 15:10:37  ...
argh cfeb RDP: Remote side reset connection:
rdp.(scb:17408).(serverRouter:chassis)

Message from syslogd@host cfeb at Jan 28 15:10:37  ...
argh cfeb RDP: Remote side reset connection: rdp.(scb:17409).(serverRouter:pfe)

Message from syslogd@host cfeb at Jan 28 15:10:37  ...
argh cfeb CM: ALARM SET: (Major) RE chassis socket closed abruptly
Complete. The local routing engine becomes the master.
```

Displaying HCM Alarms

If a single HCM installed in a routing platform fails, no alarm can be sent. However, if it is a dual system, the following alarm is displayed when the backup Routing Engine takes over.

Action To view an HCM alarm when the backup Routing Engine takes over, use the following CLI command:

user@host> **show chassis alarms**

Sample Output

```
user@host> show chassis alarms
1 alarm currently active
Alarm time               Class  Description
2005-02-16 22:10:27 UTC  Minor  Backup RE Active
```

Verifying HCM Failure

Action To view current HCM status when the backup Routing Engine takes over, use the following CLI command.

user@host> **show chassis routing-engine**

Sample Output

```
user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Master (default)
    Temperature                 33 degrees C / 91 degrees F
    DRAM                      2048 MB
    Memory utilization          13 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     0 percent
      Interrupt                  0 percent
      Idle                     100 percent
```

```
    Model                          RE-3.0
    Serial ID                      P10865703096
    Start time                     2005-02-16 22:13:19 UTC
    Uptime                        2 hours, 13 minutes, 57 seconds
Routing Engine status:
  Slot 1:
    Current state                  Master
    Election priority              Backup (default)
    Temperature                 33 degrees C / 91 degrees F
    CPU temperature             29 degrees C / 84 degrees F
    DRAM                      2048 MB
    Memory utilization          12 percent
    CPU utilization:
      User                       0 percent
      Background                 0 percent
      Kernel                     3 percent
      Interrupt                  0 percent
      Idle                      97 percent
    Model                          RE-3.0
    Serial ID                      P10865701255
    Start time                     2005-02-03 03:13:39 UTC
    Uptime                        13 days, 21 hours, 12 minutes, 35 seconds
    Load averages:                 1 minute   5 minute  15 minute
                                       0.00       0.03       0.01
```

What It Means The Routing Engine in slot RE0 and companion HCM in slot HCM0 are backup. The Routing Engine in slot RE1 and companion HCM in slot HCM1 are master.

Alternative Method To verify an HCM failure, you can also use the following CLI command:

user@host> **show chassis environment hcm**

Sample Output

```
user@host> show chassis environment hcm
HCM 0 status:
  State                          Offline
  FPGA Revision               27
HCM 1 status:
  State                          Online Master
  FPGA Revision               27
```

What It Means The HCM in slot HCM0 is offline. The HCM in slot HCM1 has taken over as master.

Performing a Swap Test on an HCM

Action To perform a swap test on a HCM, see “Performing A Swap Test” on page 438.

Returning an HCM

Action To return an HCM, find the serial number ID label (see “Locate the HCM Serial Number ID Label” on page 442), then follow the procedure as described in the *M10i Internet Router Hardware Guide,* or see “Return the Failed Component” on page 86.

Part 11

Appendices

Appendix A

Command-Line Interface Overview

This chapter provides an overview of the JUNOS software command-line interface (CLI). For more detailed information about using the JUNOS software CLI, see the *JUNOS System Basics Configuration Guide* and the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

The CLI is the interface to the software that you use whenever you access the router—whether from the console or through a remote network connection. The CLI, which automatically starts after the router finishes booting, provides commands that you use to perform various tasks, including configuring the JUNOS software, and monitoring and troubleshooting the software, network connectivity, and the router hardware.

The CLI has two modes:

- CLI Operational Mode on page 633
- CLI Configuration Mode on page 639

CLI Operational Mode

In operational mode you enter commands to monitor and troubleshoot the software, network connectivity, and router by entering commands.

When you log in to the router and the CLI starts, you are at the top level of the CLI operational mode. At this level, there are several broad groups of CLI commands (see Table 133).

Table 133: CLI Operational Mode Top-Level Commands

Command	Description
clear	Clear statistics and protocol database information. Syntax: clear <arp | bfd | bgp | firewall | helper | igmp | ike | ilmi | interfaces | ipv6 | isis | ldp | log | mld | mpls | msdp | multicast | ospf | pim | rip | ripng | route | rsvp | services | snmp | system | vrrp>
configure	Enter CLI configuration mode. Alternative commands: configure <exclusive | private>

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>file</td><td>Perform file manipulation operations, such as copy, delete, list, rename, and show.
Syntax: file <archive source destination | compare | compress source destination | copy | delete | list | rename | show></td></tr>
<tr><td>help</td><td>Provide help information.
Syntax: help <reference | syslog | topic></td></tr>
<tr><td>monitor</td><td>Monitor a log file or interface traffic in real time.
Syntax: monitor <interface> <start | stop | list> <traffic></td></tr>
<tr><td>mtrace</td><td>Display trace information about a multicast path from a source to a receiver.
Syntax: mtrace <source-name> <from-source | monitor | to-gateway></td></tr>
<tr><td>ping</td><td>Verify IP connectivity to another IP host or Asynchronous Transfer Mode (ATM) connectivity (ping ATM) using Operation Administration and Maintenance (OAM) cells to an ATM endstation.
Syntax: ping *host-name* <interface *source-interface*> <bypass-routing> <count requests> <detail> <do-not-fragment> <inet | inet6> <interval seconds> <logical-router *logical-router-name*> <loose-source value> <pattern string> <rapid> <record-route> <routing-instance *routing-instance-name*> <size bytes> <strict strict-source value> <tos type-of-service> <ttl value> <verbose> <via route> <wait seconds>
Syntax: ping atm interface *interface* <count *count*> <end-to-end | segment> <interval *interval*> <sequence-number *sequence-number*> <vci *vci*> <brief>
Syntax: ping vpn-interface *vpn-interface host* <local *echo-address*></td></tr>
<tr><td>pipe</td><td>Filter the output of an operational mode or configuration mode command.
Syntax: | *<compare <filename | rollback n> | count | display <detail | inheritance | xml> | except pattern | find pattern | hold | last | match pattern | no-more | resolve <full-names> | save filename | trim columns>*</td></tr>
<tr><td>quit</td><td>Log out from the CLI process.
Syntax: quit</td></tr>
<tr><td>request</td><td>■ Stop or reboot router components, switch between primary and backup components, display messages, and display system information.
Syntax: request <chassis | ipsec switch | message | routing-engine | security | services flow-collector | support information>
■ Stop or reboot the router, load software packages, and back up the router’s file systems.
Syntax: request <chassis | ipsec switch | message | routing-engine | security | services</td></tr>
<tr><td>restart</td><td>Restart the router hardware or software processes.
Syntax: restart <adaptive-services | chassis-control | class-of-service | disk-monitoring | ecc-error-logging | firewall | interface-control | kernel-replication | l2tp-service | mib-process | network-access-service | pgm | pic-services-logging | remote-operations routing | sampling | snmp> <gracefully | immediately | soft></td></tr>
<tr><td>set</td><td>Set CLI properties, the router’s date and time, and the craft interface display text.
Syntax: set <chassis | cli | date | date ntp></td></tr>
</table>

Command	Description
show	Show information about all aspects of the software, including interfaces and routing protocols. Syntax: show <accounting | aps | arp | as-path | bgp | chassis | class-of-service | cli | configuration | connections | dvmrp | firewall | helper | host | igmp | ike | ilmi | interfaces | ipsec | ipv6 | isis | l2circuit | l2vpn | ldp | link-management | log | mpls | msdp | multicast | ntp | ospf | ospf3 | passive monitoring | pfe | pim | policer | policy | rip | ripng | route | rsvp | sap | services | snmp | system | task | ted | version | vrrp>
ssh	Open a secure shell to another host. Syntax: ssh *host-name* <bypass-routing> <interface *interface-name*> <inet | inet6> <routing instance *routing-instance-name*> <source *source-name*> <v1 | v2> <vpn-interface *vpn-interface-name*>
start	Start a software process. Syntax: start shell
telnet	Start a telnet session to another host. Syntax: telnet *host-name* <8bit> <bypass-routing> < inet | inet6> <interface *interface-name*> <logical-router *logical-router-name*> <noresolve> <port *port-number*> <routing-instance *routing-instance-name*> <source *source-address*>
test	Run various diagnostic debugging commands. Syntax: test configuration (filename | terminal)
traceroute	Trace the route to a remote host. Syntax: traceroute *host-name* <as-number-lookup> <bypass-routing> <gateway address> <inet><inet6> <logical-router *logical-router-name*> <noresolve> <routing-instance *routing-instance-name*> <source address> <tos value> <ttl value> <interface *interface-name*> <wait *seconds*>

Using the CLI Operational Mode

This section describes how to use the CLI operational mode. You can do the following:

- Entering the CLI Operational Mode on page 636
- Getting Help on Commands at a Hierarchy Level on page 636
- Getting Help About Commands on page 636
- Having the CLI Complete Commands on page 638
- Using CLI Command Completion on page 638
- Displaying CLI Command History on page 639

Entering the CLI Operational Mode

To enter the JUNOS software CLI, use the following command:

user@host> **cli**

You are in the CLI when you see the > prompt, which is preceded by a string that defaults to the name of the user and the name of the router. For example:

user@host>

Getting Help on Commands at a Hierarchy Level

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

To get help while in the CLI, type ?. You do not need to press Enter after typing the question mark. You have the following options:

- If you type the question mark at the command-line prompt, the CLI lists the available commands and options.
- If you type the question mark after entering the complete name of a command or command option, the CLI lists the available commands and options, then redisplays the command names and options that you typed.
- If you type the question mark in the middle of a command name, the CLI lists possible command completions that match the letters you have entered so far, then redisplays the letters that you typed.

Getting Help About Commands

To get help about operational mode CLI commands, you can do the following:

- Listing Top-Level Operational Mode CLI Commands on page 637
- Listing CLI Commands That Start with a Particular Letter on page 637
- Listing All Available Commands of a Particular Type on page 637

Listing Top-Level Operational Mode CLI Commands

To list all available commands at the top level of the CLI operational mode, use the following command (see Table 133):

user@host> **?**

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

Listing CLI Commands That Start with a Particular Letter

To list all commands that start with the letter c, use the following CLI command:

user@host> **c?**

```
Possible completions:
  clear                     Clear information in the system
  configure                 Manipulate software configuration information
user@host> c
```

Listing All Available Commands of a Particular Type

To list all available clear commands, use the following CLI command:

user@host> **clear ?**

```
Possible completions:
  arp                  Clear address resolution information
  bfd                  Clear Bidirectional Forwarding Detection information
  bgp                  Clear Border Gateway Protocol information
  cli                  Clear command-line interface settings
  esis                 Clear end system-to-intermediate system information
  firewall             Clear firewall counters
  helper               Clear port-forwarding helper information
  igmp                 Clear Internet Group Management Protocol information
  ike                  Clear IKE information
  ilmi                 Clear interim local management interface statistics
  interfaces           Clear interface information
  ipsec                Clear IP Security information
  ipv6                 Clear IP version 6 information
  isis                 Clear Intermediate System-to-Intermediate System
information
  ldp                  Clear Label Distribution Protocol information
  log                  Clear contents of log file
```

```
  mld                    Clear multicast listener discovery information
  mpls                   Clear Multiprotocol Label Switching information
  msdp                   Clear Multicast Source Discovery Protocol information
  multicast              Clear multicast information
  ospf                   Clear Open Shortest Path First information
  ospf3                  Clear Open Shortest Path First version 3 information
  pgm                    Clear Pragmatic Generalized Multicast information
  pim                    Clear Protocol Independent Multicast information
  rip                    Clear Routing Information Protocol information
  ripng                  Clear Routing Information Protocol for IPv6 information
  rsvp                   Clear Resource Reservation Protocol information
  services
  snmp                   Clear Simple Network Management Protocol information
  system                 Clear system information
  vpls                   Clear VPLS information
  vrrp                   Clear Virtual Router Redundancy Protocol statistics
```

Having the CLI Complete Commands

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

To complete a command or option that you have partially typed, press the Tab key or the spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command, and the possible completions are displayed.

Command completion also applies to other strings, such as filenames and usernames. To display all possible values, type a partial string followed by a question mark. However, to complete these strings, press the Tab key; pressing the space bar does not work.

Using CLI Command Completion

To complete the show interfaces command, do the following:

user@host> **show in<Spacebar>**terfaces **<Enter>**

```
Physical interface: at-0/1/0, Enabled, Physical link is Up
  Interface index: 11, SNMP ifIndex: 65
  Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode
  Speed: OC12, Loopback: None, Payload scrambler: Enabled
  Device flags   : Present Running
  Link flags     : 0x01
[...Output truncated...]
```

To display a list of all log files whose names start with the string "messages," and then display the contents of one of the files, do the following:

user@host> **show log mes?**

```
Possible completions:
  <filename>                    Log file to display
  messages                      Size: 1417052, Last changed: Mar  3 00:33
  messages.0.gz                 Size: 145575, Last changed: Mar  3 00:00
  messages.1.gz                 Size: 134253, Last changed: Mar  2 23:00
  messages.10.gz                Size: 137022, Last changed: Mar  2 14:00
  messages.2.gr                 Size: 137112, Last changed: Mar  2 22:00
  messages.3.gz                 Size: 121633, Last changed: Mar  2 21:00
  messages.4.gz                 Size: 135715, Last changed: Mar  2 20:00
  messages.5.gz                 Size: 137504, Last changed: Mar  2 19:00
  messages.6.gz                 Size: 134591, Last changed: Mar  2 18:00
  messages.7.gz                 Size: 132670, Last changed: Mar  2 17:00
  messages.8.gz                 Size: 136596, Last changed: Mar  2 16:00
  messages.9.gz                 Size: 136210, Last changed: Mar  2 15:00

user@host> show log mes<Tab>sages.4<Tab>.gz<Enter>
Jan 15 21:00:00 myhost newsyslog[1381]: logfile turned over
[...Output truncated...]
```

Displaying CLI Command History

You can display a list of recent commands that you issued. To display the command history, use the show cli history command:

user@host> **show cli history**

```
03-03 01:00:50 -- show cli history
03-03 01:01:12 -- show interfaces terse
03-03 01:01:22 -- show interfaces lo0
03-03 01:01:44 -- show bgp next-hop-database
03-03 01:01:51 -- show cli history
```

By default, this command displays the last 100 commands issued in the CLI. Specify a number with the command to display that number of recent commands. For example:

user@host> **show cli history 3**

01:01:44 – show bgp next-hop-database

```
01:01:51 -- show cli history
01:02:51 -- show cli history 3
```

CLI Configuration Mode

In configuration mode, you configure the JUNOS software by creating a hierarchy of configuration statements. You can do this by using the CLI or by creating a text (ASCII) file that contains the statement hierarchy. (The statement hierarchy is identical in both the CLI and text configuration file.) You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties. When you have finished entering the configuration statements, you commit them, which activates the configuration on the router.

Table 134 explains each CLI configuration mode command. The commands are organized alphabetically.

Table 134: CLI Configuration Mode Commands

Command	Description
activate	Remove the inactive: tag from a statement, effectively reading the statement or identifier to the configuration. Statements or identifiers that have been activated take effect when you next issue the commit command. Syntax: activate (*statement-path* | *identifier*)
annotate	Add comments to a configuration. Syntax: annotate *statement-path* "*comment-string*"
commit	Commit the set of changes to the database and cause the changes to take operational effect. Syntax: commit <<at <*string*>> <and-quit> <check> <confirmed <*minutes*>> <synchronize>
copy	Make a copy of an existing statement in the configuration. Syntax: copy *existing-statement-path* to *new-statement-path*
deactivate	Add the inactive: tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the commit command. Syntax: deactivate (*statement-path* | *identifier*)
delete	Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it. Syntax: delete (*statement-path* | i*dentifier*)
edit	Move inside the specified statement hierarchy. If the statement does not exist, it is created. Syntax: edit *statement-path*
exit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms. Syntax: exit (configuration-mode)
help	Display help about available configuration statements. Syntax: help (apropos | topic | reference) <*string*>
insert	Insert an identifier into an existing hierarchy. Syntax: insert (*statement-path*) *identifier1* (before | after) *identifier2*
load	Load a configuration from an ASCII configuration file or from terminal input. Your current location in the configuration hierarchy is ignored when the load operation occurs. Syntax: load (merge | override | patch | replace) (*filename* | terminal)
quit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms. Syntax: quit configuration-mode
rename	Rename an existing configuration statement or identifier. Syntax: rename <*statement-path*> *identifier1* to *identifier2*

Command	Description
rollback	Return to a previously committed configuration. The software saves the last 10 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command. rollback 0 erases any configuration changes made to the current candidate configuration. The currently operational JUNOS software configuration is stored in the file juniper.conf, and the last three committed configurations are stored in the files juniper.conf.1.gz, juniper.conf.2.gz, and juniper.conf.3.gz. These four files are located in the directory /config/, which is on the router's flash drive. The remaining six previous committed configurations, the files juniper.conf.4.gz through juniper.conf.9.gz, are stored in the directory /var/db/config/, which is on the router's hard disk. Syntax: rollback <*number*>
run	Run a CLI command without exiting from configuration mode. Syntax: run *command*
save	Save the configuration to an ASCII file, by default in the users home directory. The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy. Syntax: save *filename*
set	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change, and you can set identifier values whereas edit only allows access to a statement-path. Syntax: set (*statement-path* | *identifier)*
show	Display the current configuration. Syntax: show (*statement-path* | *identifier)*
status	Display the users currently editing the configuration.
top	Return to the top level of configuration command mode, which is indicated by the [edit] banner, or execute a command from the top level of the configuration. Syntax: top <*configuration-command*>
up	Move up one level in the statement hierarchy. Syntax: up <*number*>
update	Update a private database.

Configuration Statements and Identifiers

You configure all router properties by including statements in the configuration. A statement consists of a keyword, which is fixed text, and, optionally, an identifier. An identifier is an identifying name that you define, such as the name of an interface, or a username, which allows you and the CLI to discriminate among a collection of statements.

The following list shows the statements available at the top level of the configuration mode (that is, the trunk of the hierarchy tree). Table 135 on page 642 describes each statement.

```
[edit]
user@host# set ?
Possible completions:
> access                  Network access configuration
```

```
> accounting-options   Accounting data configuration
> applications         Define applications by protocol characteristics
+ apply-groups         Groups from which to inherit configuration data
> chassis              Chassis configuration
> class-of-service     Class-of-service configuration
> firewall             Define a firewall configuration
> forwarding-options   Configure options to control packet sampling
> groups               Configuration groups
> interfaces           Interface configuration
> isdn                 ISDN process configuration
> logical-routers      Logical routers
> policy-options       Routing policy option configuration
> protocols            Routing protocol configuration
> routing-instances    Routing instance configuration
> routing-options      Protocol-independent routing option configuration
> security             Security configuration
> services             Service PIC applications settings
> snmp                 Simple Network Management Protocol configuration
> system               System parameters
```

An angle bracket (>) before the statement name indicates that it is a container statement and you can define other statements at levels below it.

If there is no angle bracket (>) before the statement name, the statement is a leaf statement; you cannot define other statements at hierarchy levels below it.

A plus sign (+) before the statement name indicates that it can contain a set of values. To specify a set, include the values in brackets. For example:

[edit]
user@host# **set policy-options community my-as1-transit members [65535:10 65535:11]**

In some statements, you can include an identifier. For some identifiers, such as interface names, you must specify the identifier in a precise format. For example, the interface name so-0/0/0 refers to a SONET/SDH interface that is on the Flexible PIC Concentrator (FPC) in slot 0, in the first Physical Interface Card (PIC) location, and in the first port on the PIC. For other identifiers, such as interface descriptive text, policy, and firewall term names, you can specify any name, including special characters, spaces, and tabs.

You must enclose in quotation marks (double quotes) identifiers and any strings that include the following characters: space tab ( ) [ ] { } ! @ # $ % ^ & | ' = ?

Table 135 describes each top-level CLI configuration mode statement.

Table 135: Configuration Mode Top-Level Statements

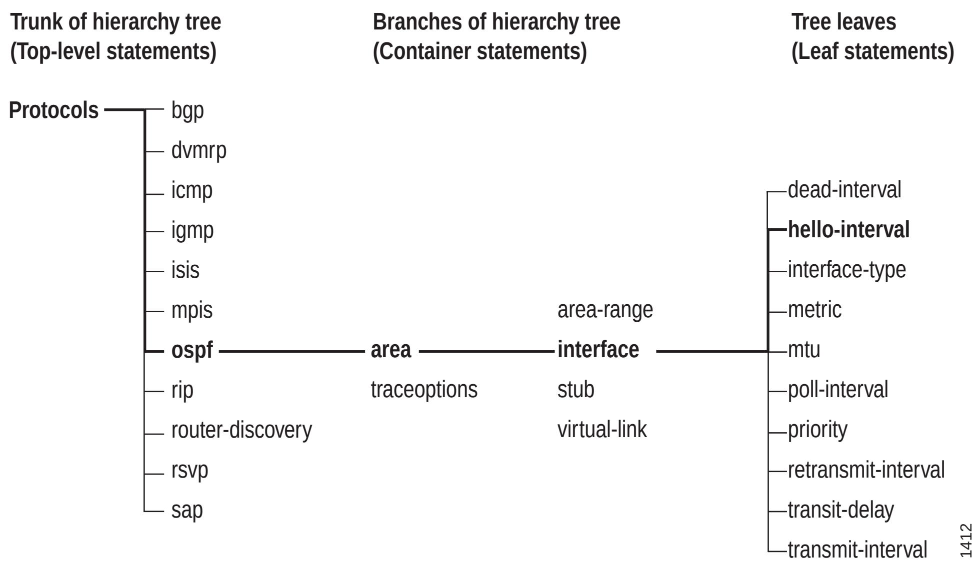
Statement	Description
accounting-options	Configure accounting statistics data collection for interfaces and firewall filters. For information about the statements in this hierarchy, see the *JUNOS Configuration Guide: Network Management*.
chassis	Configure properties of the router chassis, including the clock source, conditions that activate alarms, and SONET/SDH framing and concatenation properties. For information about the statements in this hierarchy, see the *JUNOS Interfaces and Class of Service .Configuration Guide*

Statement	Description
class-of-service	Configure class-of-service parameters. For information about the statements in this hierarchy, see the *JUNOS Interfaces and Class of Service Configuration Guide*.
firewall	Define filters that select packets based on their contents. For information about the statements in this hierarchy, see the *Policy Framework Configuration Guide*.
forwarding-options	Define forwarding options, including traffic sampling options. For information about the statements in this hierarchy, see the *JUNOS Interfaces and Class of Service Configuration Guide*.
groups	Configure configuration groups.
interfaces	Configure interface information, such as encapsulation, interfaces, virtual channel identifiers (VCIs), and data-link channel identifiers (DLCIs). For information about the statements in this hierarchy, see the *JUNOS Interfaces and Class of Service Configuration Guide*.
policy-options	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes. For information about the statements in this hierarchy, see the *JUNOS Routing and Routing Protocols Configuration Guide*.
protocols	Configure routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP), and Resource Reservation Protocol (RSVP). For information about the statements in this hierarchy, see the chapters that discuss how to configure the individual routing protocols in the *JUNOS Routing and Routing Protocols Configuration Guide* and the *JUNOS MPLS Applications Configuration Guide*.
routing-instances	Configure multiple routing instances. For information about the statements in this hierarchy, see the *JUNOS Routing and Routing Protocols Configuration Guide*.
routing-options	Configure protocol-independent routing options, such as static routes, autonomous system (AS) numbers, confederation members, and global tracing (debugging) operations to log. For information about the statements in this hierarchy, see the *JUNOS Routing and Routing Protocols Configuration Guide*.
snmp	Configure Simple Network Management Protocol (SNMP) community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the *JUNOS Network Management Configuration Guide*.
system	Configure systemwide properties, including the hostname, domain name, Domain Name System (DNS) server, user logins and permissions, mappings between hostnames and addresses, and software processes.

Configuration Statement Hierarchy

The JUNOS software configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not contain other statements (see Figure 235). All of the container and leaf statements together form the *configuration hierarchy*.

Figure 235: Configuration Mode Hierarchy of Statements



Each statement at the top level of the configuration hierarchy resides at the trunk (or root level) of a hierarchy tree. The top-level statements are container statements, containing other statements that form the tree branches. The leaf statements are the leaves of the hierarchy tree. An individual hierarchy of statements, which starts at the trunk of the hierarchy tree, is called a *statement path*. Figure 235 illustrates the hierarchy tree, showing a statement path for the portion of the protocol configuration hierarchy that configures the hello interval on an interface in an OSPF area.

The protocols statement is a top-level statement at the trunk of the configuration tree. The ospf, area, and interface statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree), and the hello-interval statement is a leaf on the tree, which, in this case, contains a data value: the length of the hello interval in seconds.

The CLI represents the statement path shown in Figure 235 as [protocols ospf area *area-number* interface *interface-name*], and displays the configuration as follows:

```
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0 {
                hello-interval 5;
            }
            interface so-0/0/1 {
                hello-interval 5;
            }
        }
    }
}
```

The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed. Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon.

The CLI uses this indented representation when it displays the current system configuration, and you use this format when creating ASCII files that contain the software configuration. However, the format of ASCII configuration files is not as strict as the CLI output of the configuration. Although the braces and semicolons are required, the indentation and use of new lines, as shown above, are not required in ASCII configuration files.

Using the CLI Configuration Mode

This section describes how to use the CLI configuration mode. You can do the following:

- Returning to a Previously Committed Configuration on page 651
- Getting Help About Statements on page 653

Entering Configuration Mode

If many users enter configuration mode at the same time, everyone can make configuration changes and commit all changes. If one user enters configuration mode when another user is also in configuration mode, a message indicates who the user is and what portion of the configuration that user is viewing or editing. To enter configuration mode, use the following CLI command:

user@host> **configure**

```
Entering configuration mode
Current configuration users:
    root terminal p3 (pid 1088) on since 1999-05-13 01:03:27 EDT
        [edit interfaces so-3/0/0 unit 0 family inet]
The configuration has been changed but not committed
```

- If, when you enter configuration mode, the configuration contains changes that have not been committed, a message appears:

  user@host> **configure**

  ```
  Entering configuration mode
  The configuration has been changed but not committed
  ```

- If, while in configuration mode, you try to make a change while the configuration is locked by another user, a message indicates that the configuration database is locked, who the user is, and what portion of the configuration the user is viewing or editing:

  [edit]
  user@host# **set system host-name ipswitch**

  ```
  error: configuration database locked by:
      user2 terminal d0 (pid 1828) on since 19:47:58 EDT, idle 00:02:11
          exclusive [edit protocols]
  ```

- If you enter configuration mode with the configure exclusive command, you lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. If another user is also in configuration mode and has the configuration locked, a message indicates who the user is and what portion of the configuration the user is viewing or editing:

  user@host> **configure exclusive**

  ```
  Entering configuration mode
  Users currently editing the configuration:
      root terminal p3 (pid 1088) on since 2000-10-30 19:47:58 EDT, idle
  00:00:44
      exclusive [edit interfaces so-3/0/0 unit 0 family inet]
  ```

Exiting Configuration Mode

To exit configuration mode, use the exit configuration-mode configuration mode command from any level or use the exit command from the top level. If you try to exit from configuration mode using the exit command and the configuration contains changes that have not been committed, you see a message and prompt:

```
[edit]
user@host# exit

The configuration has been changed but not committed
Exit with uncommitted changes? [yes,no] (yes) <Enter>
Exiting configuration mode
user@host>
```

To exit with uncommitted changes without having to respond to a prompt, use the exit configuration-mode command.

Moving Among Levels of the Hierarchy

The CLI commands in Table 136 help you navigate the levels of the configuration statement hierarchy.

Table 136: CLI Configuration Mode Navigation Commands

Command	Description
edit	To move down through an existing configuration command hierarchy, or to create a hierarchy and move down to that level, use the edit configuration mode command, specifying the hierarchy level at which you want to be.
exit	To move up the hierarchy, use the exit configuration mode command. This command is, in effect, the opposite of the edit command.
up	To move up the hierarchy one level at a time, use the up configuration mode command.
top	To move directly to the top level, use the top configuration mode command.

Displaying the Current Configuration

You can display the following information about the current configuration:

- Displaying the Configuration at the Current Hierarchy Level on page 648
- Displaying the Last Committed Current Configuration on page 648
- Displaying Users Currently Editing the Configuration on page 648

Displaying the Configuration at the Current Hierarchy Level

To display the configuration at the current hierarchy level or at the specified level, use the show configuration mode command.

user@host> **show** <*statement-path*>

The configuration statements appear in a fixed order. The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed. Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon. Interfaces appear alphabetically by type, and then in numerical order by slot number, PIC number, and port number.

Displaying the Last Committed Current Configuration

You also can use the CLI operational mode show configuration command to display the last committed current configuration, which is the configuration currently running on the router:

user@host> **show configuration**

Displaying Users Currently Editing the Configuration

To display the users currently editing the configuration, use the status configuration mode command:

[edit]
user@host# **status**

```
Current configuration users:
  user terminal p0 (pid 518) on since 2002-03-12 18:24:27 PST
      [edit protocols]
```

The system displays who is editing the configuration (user), how the user is logged in (terminal p0), the date and time the user logged in (2002-03-12 18:24:27 PST), and what level of the hierarchy the user is editing ([edit protocols]).

Modifying the Configuration

To configure the router or to modify an existing router configuration, you add statements to the configuration. For each statement hierarchy, you create the hierarchy starting with a statement at the top level and continuing with statements that move progressively lower in the hierarchy.

To modify the hierarchy, you use two configuration mode commands:

- set—Creates a statement hierarchy and sets identifier values. After you issue a set command, you remain at the same level in the hierarchy. The set command has the following syntax:

  set <*statement-path*> *statement* <*identifier*>

  statement-path is the hierarchy to the configuration statement and the statement itself. If you have already moved to the statement's hierarchy level, you omit this. *statement* is the configuration statement itself. *identifier* is a string that identifies an instance of a statement.

- edit—Moves to a particular hierarchy level. If that hierarchy level does not exist, the edit command creates it and then moves to it. The edit command has the following syntax:

  edit <*statement-path*> *statement* <*identifier*>

Removing a Statement

To delete a statement or identifier, use the delete configuration mode command. Deleting a statement or an identifier effectively "unconfigures" the functionality associated with that statement or identifier, returning that functionality to its default condition. When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration.

delete <*statement-path*> <*identifier*>

To delete the entire hierarchy starting at the current hierarchy level, do not specify a statement or an identifier in the delete command:

[edit]
user@host# **delete**

```
Delete everything under this level? [yes, no] (no) ?
    Possible completions:
        no          Don't delete everything under this level
        yes         Delete everything under this level
Delete everything under this level? [yes, no] (no)
```

Running Operational Mode CLI Commands from Configuration Mode

To display the output of an operational mode show or other command while configuring the software, you can execute a single operational mode command by issuing the run configuration mode command and specifying the operational mode command:

[edit]
user@host# **run** *operational-mode-command*

Displaying Configuration Mode Command History

To display a list of the recent commands you issued while in configuration mode, use the run show cli history command. By default, this command displays the last 100 commands issued in the CLI.

```
[edit]
user@host# run show cli history
```

```
12:40:08 -- show
12:40:17 -- edit protocols
12:40:27 -- set isis
12:40:29 -- edit isis
12:40:40 -- run show cli history
```

Committing a Configuration

To commit a configuration, you can do the following:

Saving Configuration Changes and Activating the Configuration

To save software configuration changes to the configuration database and activate the configuration on the router, use the commit configuration mode command:

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

```
commit complete
```

The configuration is checked for syntax errors. If the syntax is correct, the configuration is activated and becomes the current, operational router configuration. If the configuration contains syntax errors, a message indicates the location of the error and the configuration is not activated. You must correct the error before recommitting the configuration.

Saving Configuration Changes, Activating the Configuration, and Exiting Configuration Mode

To save software configuration changes, activate the configuration on the router, and exit configuration mode, use the commit and-quit configuration mode command. This command succeeds only if the configuration contains no errors.

```
[edit]
user@host# commit and-quit
```

```
commit complete
exiting configuration mode
user@host>
```

Saving a Configuration to a File

To save the configuration to a text (ASCII) file so that you can edit it with a text editor of your choice, use the save configuration mode command. By default, the configuration is saved to that file in your home directory, which is on the flash disk.

```
[edit]
user@host# save filename
Wrote 475 lines of configuration to 'filename'
```

Returning to a Previously Committed Configuration

To return to a previously committed configuration, you can do the following:

- Returning to the Most Recently Committed Configuration on page 651
- Activating the Configuration You Loaded on page 651
- Returning to a Configuration Prior to the Most Recently Committed One on page 651
- Displaying Previous Configurations on page 652

Returning to the Most Recently Committed Configuration

To return to the most recently committed configuration and load it into configuration mode without activating it, use the rollback configuration mode command:

```
[edit]
user@host# rollback
```

```
load complete
```

Activating the Configuration You Loaded

To activate the configuration that you loaded, use the commit command:

```
[edit]
user@host# rollback
load complete
[edit]
user@host# commit
```

Returning to a Configuration Prior to the Most Recently Committed One

To return to a configuration prior to the most recently committed one, include the number in the rollback command. *number* can be a number in the range 0 through 9. The most recently saved configuration is number 0 (which is the default configuration to which the system returns), and the oldest saved configuration is number 9.

```
[edit]
user@host# rollback number
load complete
```

Displaying Previous Configurations

To display previous configurations, including the rollback number, date, time, the name of the user who committed changes, and the method of commit, use the rollback ? command.

```
[edit]
user@host# rollback ?
```

```
Possible completions:
<[Enter]> Execute this command
<number> Numeric argument
  0                    2005-02-27 12:52:10 PST by abc via cli
  1                    2005-02-26 14:47:42 PST by def via cli
  2                    2005-02-14 21:55:45 PST by ghi via cli
  3                    2005-02-10 16:11:30 PST by jkl via cli
  4                    2005-02-10 16:02:35 PST by mno via cli
  5                    2005-03-16 15:10:41 PST by pqr via cli
  6                    2005-03-16 14:54:21 PST by stu via cli
  7                    2005-03-16 14:51:38 PST by vwx via cli
  8                    2005-03-16 14:43:29 PST by yzz via cli
  9                    2005-03-16 14:15:37 PST by abc via cli
  10                   2005-03-16 14:13:57 PST by def via cli
  11                   2005-03-16 12:57:19 PST by root via other
  12                   2005-03-16 10:45:23 PST by root via other
  13                   2005-03-16 10:08:13 PST by root via other
  14                   2005-03-16 01:20:56 PST by root via other
  15                   2005-03-16 00:40:37 PST by ghi via cli
  16                   2005-03-16 00:39:29 PST by jkl via cli
  17                   2005-03-16 00:32:36 PST by mno via cli
  18                   2005-03-16 00:31:17 PST by pqr via cli
  19                   2005-03-15 19:59:00 PST by stu via cli
  20                   2005-03-15 19:53:39 PST by vwx via cli
  21                   2005-03-15 18:07:19 PST by yzz via cli
  22                   2005-03-15 17:59:03 PST by abc via cli
  23                   2005-03-15 15:05:14 PST by def via cli
  24                   2005-03-15 15:04:51 PST by ghi via cli
  25                   2005-03-15 15:03:42 PST by jkl via cli
  26                   2005-03-15 15:01:52 PST by mno via cli
  27                   2005-03-15 14:58:34 PST by pqr via cli
  28                   2005-03-15 13:09:37 PST by root via other
  29                   2005-03-12 11:01:20 PST by stu via cli
  30                   2005-03-12 10:57:35 PST by vwx via cli
  31                   2005-03-11 10:25:07 PST by yzz via cli
  32                   2005-03-10 23:40:58 PST by abc via cli
  33                   2005-03-10 23:40:38 PST by def via cli
  34                   2005-03-10 23:14:27 PST by ghi via cli
  35                   2005-03-10 23:10:16 PST by jkl via cli
  36                   2005-03-10 23:01:51 PST by mno via cli
  37                   2005-03-10 22:49:57 PST by pqr via cli
  38                   2005-03-10 22:24:07 PST by stu via cli
  39                   2005-03-10 22:20:14 PST by vwx via cli
  40                   2005-03-10 22:16:56 PST by yzz via cli
  41                   2005-03-10 22:16:41 PST by abc via cli
  42                   2005-03-10 20:44:00 PST by def via cli
  43                   2005-03-10 20:43:29 PST by ghi via cli
  44                   2005-03-10 20:39:14 PST by jkl via cli
  45                   2005-03-10 20:31:30 PST by root via other
  46                   2005-03-10 18:57:01 PST by mno via cli
  47                   2005-03-10 18:56:18 PST by pqr via cli
  48                   2005-03-10 18:47:49 PST by stu via cli
  49                   2005-03-10 18:47:34 PST by vw via cli
```

```
|   Pipe through a command
[edit]
```

Getting Help About Statements

In configuration mode, you can use the help command to display help based on a text string contained in a statement name. This command displays help for statements at the current hierarchy level and below.

user@host# **help** *string*

You can also display help based on a text string contained in a statement name using the help topic and help reference commands. The help topic command displays usage guidelines for the statement, whereas the help reference command displays summary information about the statement.

```
user@host# help topic ?
  access               Network access control
  accounting-options   Accounting data collection
  applications         Application protocols
  bgp                  Border Gateway Protocol
  chassis              Platform
  class-of-service     Class of service (CoS)
  connections          Circuit cross-connect (CCC)
  dvmrp                Distance Vector Multicast Routing Protocol
  firewall             Firewalls and filters
  forwarding-options   Packet sampling
  groups               Configuration groups
  igmp                 Internet Group Management Protocol
  interfaces           Interfaces
  isis                 Intermediate System-to-Intermediate System
  l2circuit            Layer 2 virtual circuits
  layer2-vpns          Layer 2 VPNs
  layer3-vpns          Layer 3 VPNs
  ldp                  Label Distribution Protocol
  link-management      Link Management Protocol
  logical-routers      Logical routers
  mld                  Multicast Listener Discovery protocol
  mpls                 Multiprotocol Label Switching
  msdp                 Multicast Source Discovery Protocol
  ospf                 Open Shortest Path First protocol
  pgm                  Pragmatic Generalized Multicast
  pim                  Protocol-Independent Multicast and data MDT
  policy-options       Routing policy
  rip                  Routing Information Protocol
  ripng                Routing Information Protocol Next Generation
  rmon                 Remote Monitoring
  router-advertisement Neighbor discovery
  router-discovery     Internet Control Message Protocol router discovery
  routing-instances    Routing instances
  routing-options      Protocol-independent routing options
  rsvp                 Resource Reservation Protocol
  sap                  Session Advertisement Protocol
  security             Internet Protocol security (IPSec)
  services             Service sets for Adaptive Services PIC
  snmp                 Simple Network Management Protocol
  system               System parameters
```

```
  vpls                 Virtual private LAN service
  vpns                 Virtual private networks


[edit]
user@help# help topic access ?
Possible completions:
  examples
  l2tp                 Overview of Layer 2 Tunneling Protocol configuration
  point-to-point       Overview of Point-to-Point Protocol configuration
  radius-disconnect-port  Port number for RADIUS disconnect server
  radius-server        RADIUS server configuration
  traceoptions         Trace options for access processes
  tunnel-profile       Join multilink bundles based on endpoint discriminator


[edit]
user@host# help topic access point-to-point
Configuring the Point-to-Point Protocol

   To configure the Point-to-Point Protocol (PPP), do the following:
     * Configuring the Challenge Handshake Authentication Protocol

     * Configuring the Authentication Order

user@host# help reference string
```

If you do not type an option for a statement that requires one, a message indicates the type of information expected. In this example, you need to type an area number to complete the command:

```
[edit]
user@host# set protocols ospf area<Enter>

syntax error, expecting <identifier>.
```

In this example, you need to type a value for the hello interval to complete the command:

```
[edit]
user@host# set protocols ospf area 45 interface so-0/0/0
                 hello-interval<Enter>

syntax error, expecting <data>
```

If you have omitted a required statement at a particular hierarchy level, when you attempt to move from that hierarchy level or when you issue the show command in configuration mode, a message indicates which statement is missing. For example:

```
[edit protocols pim interface so-0/0/0]
user@host# top
Warning: missing mandatory statement: 'mode'
[edit]
user@host# show
protocols {
    pim {
        interface so-0/0/0 {
```

```
                priority 4;
                version 2;
                # Warning: missing mandatory statement(s): 'mode'
            }
        }
}
```

Part 12

Index

Index

C

G

H

S

T